1999-09

A critical examination of IT 21 : thinking beyond vendor-based standards

Trupp, Travis J.

Monterey, California: Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

A CRITICAL EXAMINATION OF IT-21: THINKING BEYOND VENDOR-BASED STANDARDS

by

Travis J. Trupp

September 1999

Thesis Co-Advisors: Hemant K. Bhargava
Theodore G. Lewis

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	September 1999	Master's Thesis

4. TITLE AND SUBTITLE :
A CRITICAL EXAMINATION OF IT-21: THINKING BEYOND VENDOR-BASED STANDARDS

5. FUNDING NUMBERS

6. AUTHOR(S)
Trupp, Travis J.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/ MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES
The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(maximum 200 words)* The Information Technology for the 21st Century (IT-21) policy endorses the use of a Microsoft Windows NT-based PC in a client-server environment for all Navy computing needs. The rationale given for taking this vendor-based approach towards standards is that it will lower costs and increase fleet-wide interoperability. This thesis takes a critical look at the IT-21 policy from an economic, security, availability, procurement, and practical level, and explores the role of vendor-based standards in the Navy computing architecture. It identifies the concerns or deficiencies of an architecture based on products or vendors, and offers an alternative architecture that attempts to mitigate these concerns. It finds that a vendor-based standard will not necessarily increase interoperability, and the selection of Microsoft as that standard could end up costing the Navy much more than anticipated. On first inspection, vendor-based standards make sense for the reduction of costs and the increase in interoperability. However, this ignores the power that diversity gives the end user and it ignores the pending disaster of single points of failure in Navy information systems. This thesis recommends a web-based, 3/n-tier client/server computing architecture such as one using Common Object Request Broker Architecture middleware and the Extensible Markup Language for data presentation. This architecture should make it easier and cheaper to maintain and deploy applications, allow for the dynamic nature of IT, and permit computer applications to communicate with one another no matter what operating system they are using.

14. SUBJECT TERMS
IT-21 (Information Technology for the 21st Century), Information Systems, Information Technology, Availability

15. NUMBER OF PAGES
186

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

Approved for public release; distribution is unlimited

A CRITICAL EXAMINATION OF IT-21: THINKING BEYOND VENDOR-BASED STANDARDS

Travis J. Trupp
Lieutenant, United States Navy
B.S., Oregon State University, 1991

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 1999

Author: [redacted]
Travis J. Trupp

Approved by: [redacted]
Hemant K. Bhargava, Thesis Co-Advisor

[redacted]
Theodore G. Lewis, Thesis Co-Advisor

[redacted]
Dan C. Boger, Chairman
Information Systems Academic Group

ABSTRACT

The Information Technology for the 21st Century (IT-21) policy endorses the use of a Microsoft Windows NT-based PC in a client-server environment for all Navy computing needs. The rationale given for taking this vendor-based approach towards standards is that it will lower costs and increase fleet-wide interoperability. This thesis takes a critical look at the IT-21 policy from an economic, security, availability, procurement, and practical level, and explores the role of vendor-based standards in the Navy computing architecture. It identifies the concerns or deficiencies of an architecture based on products or vendors, and offers an alternative architecture that attempts to mitigate these concerns. It finds that a vendor-based standard will not necessarily increase interoperability, and the selection of Microsoft as that standard could end up costing the Navy much more than anticipated. On first inspection, vendor-based standards make sense for the reduction of costs and the increase in interoperability. However, this ignores the power that diversity gives the end user and it ignores the pending disaster of single points of failure in Navy information systems. This thesis recommends a web-based, 3/n-tier client/server computing architecture such as one using Common Object Request Broker Architecture middleware and the Extensible Markup Language for data presentation. This architecture should make it easier and cheaper to maintain and deploy applications, allow for the dynamic nature of IT, and permit computer applications to communicate with one another no matter what operating system they are using.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGMENT

I would like to thank all those who might read this thesis, in advance, for maintaining an open mind. This thesis states concerns the author has with a vendor-based computing architecture, tries to identify deficiencies to be avoided with that standard, and offers an alternative course of action for future implementations of the Navy information system architecture. It is the author's intent to create a migration path to the next evolution of the Navy computing architecture and hopefully prevent the vendor-based standards the Navy picks today from becoming the legacy systems of tomorrow.

I would like to acknowledge the time and guidance provided by Professors Hemant Bhargava and Theodore Lewis. It was their help and advice that brought this work to full fruition. I would also like to thank Professor William Haga who provided guidance and ideas in the early stages of my thesis topic development.

Finally to my family, Carla, Gretchen, and Daniel, I want to thank you for the time you gave up when I needed to study and work. I also want you to know that without your patience and understanding this work simply would not have been possible.

I. INTRODUCTION

A. EXECUTIVE SUMMARY

The importance of the *Information Technology for the 21st Century (IT-21)* policy can not be overstated. At the time of its inception, the United States Navy did not have a coherent Information Technology (IT) policy. Increasing IT costs, an aging IT infrastructure, and frustrating problems with interoperability were troubling the fleet. In an attempt to rectify these problems, a Fleet Commander offered a solution—IT-21. The IT-21 policy established a vendor-based standard in an effort to address the cost and interoperability problems plaguing the fleet. It named Microsoft Windows NT Server 4.0 as the standard fleet Network Operating System (NOS), Microsoft Exchange as the standard e-mail solution, and Microsoft Office 97 as the standard fleet office automation system software.

Whenever a new policy is introduced and implemented in the Navy, it is often helpful to examine that policy and then project into the future to help determine what the next generation of that policy should look like. This thesis is an attempt to do just that with the IT-21 policy. A critical examination of the IT-21 policy should help to identify areas of concern or deficiencies in the Navy's current policy that can then be acted upon to help develop an improved information system architecture in the future. This thesis attempts to describe what the author believes are the main concerns or deficiencies with the IT-21 vendor-based computing standard. These deficiencies will provide the threads of the argument for alternative technologies that might prove to be better suited to the Navy's computing needs in the future. It is hoped that the ideas and alternative technologies presented in this thesis can help establish a migration path to the next evolution of the IT-21 policy.

To begin, there are several fiscal concerns associated with a vendor-based standard that do not necessarily provide the most optimal cost reduction characteristics. A homogeneous vendor-based standard makes the Navy vulnerable to high switching costs and vendor lock-in, which gives the vendor the ability to increase prices to the point that it meets the switching costs of moving to a new standard. "Lock-in can be a source of enormous headaches, or substantial profits, depending on whether you are the one stuck in the locked room or the one in possession of the key to the door." (Shapiro and Varian, 1999) Next, the selection of Microsoft as the single vendor standard carries with it a number of hidden costs in the implementation, upgrade, and licensing of those products. Many enterprises underestimate the funding required to execute a multi-server NT deployment. In fact, 90 percent are over budget, and 55 percent have exceeded their budget by at least 60 percent. (Weiss, 1997) Changes in licensing represent a 224 percent increase in prices and that is without a change in a product's list price. (Bona, 1998) The selection of this vendor-based standard locks the Navy into this standard, could potentially result in increased prices, and prevents the use of lower cost alternatives that might be better suited to the specific requirements of the end user. (Details provided in Chapter III)

Cost is not the only risk or concern facing the Navy with the selection of a vendor-based standard. There are also risks in the security of the operating system and applications selected as that standard. One of the reasons for the selection of Windows NT, and the omission of other operating systems, is the C2 security certification given by the National Security Agency. However, the standard that was picked, Windows NT version 4.0, is not C2 certified. Furthermore, the manager of security technology at the National Institute of Standards and Technology (NIST) warns that, "Government agencies—in theory—shouldn't be using NT to protect sensitive but unclassified information because it isn't FIPS 140-1 certified." (Messmer, 1999). Another problem

that affects security is Microsoft's "good enough" development strategy. Commercial of the shelf (COTS) software vendors are rewarded by time to market and ease of use, not security and availability. Microsoft's "good enough" development strategy has the potential to produce more revisions, more bugs, more security holes, and ultimately more money from the consumer—the United States Navy. (See Chapter IV for details)

On first inspection, vendor-based standards make sense for the reduction of costs and the increase in interoperability. However, this ignores the power that diversity gives the end user, the one who actually does the work. It also ignores the pending disaster of common cause failures or single points of failure in Navy information systems. Recent computer viruses/worms like Melissa and Papa that are targeted to the Microsoft operating system and Microsoft applications have been very effective in bringing homogeneous networks, reliant on these products, to a screeching halt. Furthermore, the Microsoft Windows NT operating system does not have very high user availability. Windows NT has an average availability of 97.44 percent, which translates into 224.5 hours of downtime per year. All of the other most commonly used server platforms studied in a Gartner Group survey were under 24 hours of downtime per year. (Fitzpatrick, 1998) When *diverse* and redundant systems are employed, downtime can be reduced to 42 minutes per year. (Details provided in Chapter V)

A vendor-based standard also presents difficulties in the procurement arena. To begin, sole source procurements have to be adequately justified to prevent bid protests that could slow down the procurement process. When the DOD awards 53 percent of task orders on a sole source basis without adequate justification, the military has the potential to pay more money than required for products and services, and it establishes a practice that runs counter to the spirit of competition required in the federal acquisition process. In the author's opinion, this has the potential to create sub-optimal information systems as a matter of both function and cost. (See Chapter VI for details)

Finally, there are several practical concerns associated with a vendor-based standard. To begin, strict management policies will bring costs down much more effectively than the selection of a particular vendor-based standard. Next, the lag time from standards adoption to implementation make vendor-based standards difficult to implement. With this lag time, seven generations of computer equipment will likely pass before the Navy can get technological refresh. By the time the Navy standardizes on a configuration, that configuration will probably be obsolete. In addition, a single-vendor standard is often unrealistic and ineffective. With concepts like the "Lasagna effect," the Navy will most likely have a heterogeneous computing environment, even though it standardizes on a single vendor. Finally, COTS products often require some value-added components to bring them in line with military standards, thus increasing the risk of their purchase. (Details provided in Chapter VII)

In an attempt to address the concerns or inefficiencies of a vendor-based standard, this thesis recommends standardizing at an architectural level vice at the product or vendor level. In the author's opinion, what should be of concern are the interface standards and commonality of information exchange. To deal with the inherent lag time from standards adoption to implementation in the Navy, the Navy should establish an information technology architecture that, by its very nature, promotes interoperability. The Navy should create an object-oriented architecture, like that found in the 3/n-tier client/server environment, which will scale to meet the wider usage of the enterprise. This architecture will make it easier to maintain and deploy applications, will allow for the dynamic nature of IT, and will accommodate legacy platforms until updates or replacements can be purchased. The Navy should also use middleware like CORBA and establish presentation standards using XML. (See Chapter VIII)

"The information technology world is swimming in a sea of continuous hyperchange and in emerging technologies and processes which can be costly to system

developers and business managers, if they choose to implement the wrong technology." (Taylor, 1997) In the author's opinion, the Navy should not put all of its eggs in one basket with the continuation of a single vendor-based standard. In the next generation of this policy, the Navy should create an architecture that will allow universal access, promote platform independence, minimize vendor lock-in, and utilize open standards whenever practical. The Navy should think beyond vendor-based standards if it wants to have a lasting flexible architecture that increases fleet-wide interoperability and reduces costs.

B. OBJECTIVE

The goal of this research is to examine the United States Navy *Information Technology for the 21st Century (IT-21)* policy and identify issues, concerns, or weaknesses that can be improved upon as the Navy migrates to the next evolution of its information system architecture. This thesis focuses on the economic, security, availability, procurement, and practical issues surrounding the implementation of the IT-21 policy and offers an improved information technology architecture for the Department of Defense that is cost-effective, provides fleet-wide interoperability, and is void of specific vendor products.

C. THE RESEARCH QUESTION

The primary research question is: "What would an information technology architecture look like without products, just standards, from the desktop to the mainframe, and what does the Navy need to implement such a standards-based architecture?" The subsidiary research questions are:

- What is the lag/cycle time from standards adoption to implementation for the United States Navy?
- What is the cost of ownership of Linux versus Windows NT?

- What are the security concerns associated with standardized products? Single point of failure? Availability?
- Do vendor-based procurements maximize the benefits of "full and open competition?"

D. SCOPE, METHODOLOGY, LIMITATIONS, AND ASSUMPTIONS

This study focuses on the Information Technology for the 21st Century information system standardization policy (IT-21), and the Information Technology Standards Guidance (ITSG) produced by the Department of the Navy, Chief Information Officer, Integrated Process Team. The primary concentration of study consists of a critical examination of the homogeneous vendor-based computing standard promoted by the IT-21 policy and the development of an alternative computing architecture void of products. The methodology used in this research will consist of the following steps.

- Conduct a literature search of Government regulations, magazine articles, commentary, the Internet, and other library information resources.
- Conduct an ownership examination of Linux versus Windows NT.
- Determine the lag/cycle time from standards adoption to implementation for the United States Navy.
- Determine the security implications of a single vendor standard to include availability concerns and common cause failures.
- Determine the concerns surrounding vendor-based procurements.
- Develop an information technology architecture void of products.

This research is limited to the examination of the role of vendor based standards in the Navy computing architecture. The primary assumption in this study is that the reader is familiar with the basic rudiments of information technology and its application in the Department of the Navy.

E. ORGANIZATION OF THESIS

This thesis is comprised of eight chapters.

Chapter I Introduction: The purpose of this chapter is to introduce the research topic in an executive summary, and to detail the objective, research questions, scope, methodology, limitations, assumptions, and organization of this thesis.

Chapter II Background and Review of Standards: The intent of this chapter is to provide a background and review of the Information Technology for the 21st Century (IT-21) policy and the Information Technology Standards Guidance (ITSG). In addition, the stages of information technology transition will be introduced to the reader.

Chapter III The Economics of IT-21: This chapter will examine the concepts of switching costs and vendor lock-in in a homogeneous vendor-based computing environment. It will also explore the hidden costs associated with choosing Microsoft as the Navy's vendor-based computing standard. Economic alternatives to the single vendor standard will be presented, and a comparison of Linux and Windows NT will be conducted.

Chapter IV IT-21 Security: The intent of this chapter is to discuss some of the issues surrounding the NSA C2 certification of Windows NT and detail some of NT's top security problems.

Chapter V IT-21 Availability: This chapter attempts to explain the danger a vendor-based standard poses to information system availability due to factors such as common cause failures and single points of failure in the Navy information system architecture.

Chapter VI IT-21 Procurement Issues: The intent of this chapter is to detail the competition requirements set forth in federal acquisition regulations, offer a case study that examines the use of a vendor-based standard, and highlight recent DOD acquisition practices.

Chapter VII The Practical Issues of IT-21: The intent of this chapter is to examine the practical risks associated with commercial of the shelf software, explain why

vendor-based standards do not necessarily increase interoperability, and dispel the myth of the dual platform support cost premium.

Chapter VIII Recommendations and Conclusions: The chapter attempts to aggregate and mitigate the concerns presented in the previous chapters by offering an alternative path to the next Navy information system architecture. It argues for a web-based, object-oriented computing architecture and provides the rationale for why the Navy should standardize at an interface level, with data formats and transmission protocols, vice standardizing on vendors and products.

II. BACKGROUND AND REVIEW OF STANDARDS

A. THE NEED FOR INFORMATION SYSTEMS STANDARDS

Ever since the end of World War II and the deployment of radar in the fleet, the United States Navy has searched for ways to implement battle management and increase battlespace awareness. In the early years, the goal was to detect incoming air threats and prevent kamikaze leakers from destroying ships. The Naval Tactical Data System was used to aid in this endeavor. The subsurface threat created its own set of problems and anti-submarine warfare links were added to the mix. In the 1970's, the Fleet Satellite Communications program created several new systems. The Submarine Service Information Exchange System (SSIXS) allowed communication between the submarine fleet, the Common User Information Exchange System (CUDIXS) was used for the surface fleet, the Tactical Intelligence (TACINTEL) link was used by the intelligence community, and the Officer in Tactical Command Information Exchange System (OTCIXS) was used by Navy senior leadership. These systems, among others, carried with them a host of radio frequency interference and electro-magnetic interference problems, and were mostly "stove pipe" systems. As a result, not many could "talk" to one another, causing integration and interoperability problems. As technology progressed, many sensor and shooter platforms entered service in the fleet, once again using their own "stove pipe" communication systems. These systems required many more sensors and shooters to effectively operate in a Joint combat arena. With the end of the Cold War and the resultant peace dividend, the military had to find a way to do more with less.

In the mid-1990's, Network Centric Warfare (NCW) introduced a vision that would allow the United States Navy to achieve a force capability greater than the sum of its parts. There are many elements that constitute NCW, but at its very basic level

"Network-centric warfare enables a shift from attrition-style warfare to a much faster and more effective warfighting style characterized by the new concepts of speed of command and self-synchronization." (Cebrowski and Garstka, 1998) Speed of command gives the United States military the ability to "lock-out" alternative courses of action by the enemy, and in return, "lock-in" success during wartime scenarios by achieving information superiority through increased battlespace awareness. This awareness allows the massing of effects versus the massing of forces. Self-synchronization allows the military to organize from the "bottom-up" to meet the commander's intent. With the ever-increasing limits being put on congressional appropriations for military weapon systems and platforms, the United States Navy has been forced to do more with their limited funding coffers. The "massing of effects" concept of NCW will help the United States military maintain its competitive technological and strategic advantage in battle, while meeting these reduced funding budgets. The *Information Technology for the 21st Century* policy is the technical enabler that will allow the Network Centric Warfare vision to become a reality.

B. INFORMATION TECHNOLOGY FOR THE 21ST CENTURY (IT-21)

Information Technology for the 21st Century (IT-21) is an expansive set of initiatives designed to modernize the Navy force structure through the replacement of outdated information technology (IT) equipment and related infrastructure. It is a way to remove stovepipe systems and increase interoperability while reducing the costs associated with Navy information systems. As the IT-21 policy states, "The fleets cannot continue to support a multitude of diverse operating systems and e-mail products with their own training, operational procedures and troubleshooting requirements," and as a result, "...implementation of this policy requires all non-standard NOS [Network Operating Systems] and e-mail products to be replaced NLT [No Later Than] DEC 99." (IT-21, 1997)

Microsoft Windows NT Server 4.0 was named as the standard fleet Network Operating System (NOS), Microsoft Exchange was designated as the standard e-mail solution for both fleets, and Microsoft Office 97 was designated as the standard fleet office automation system software. Compliance with this standard was so important that the policy states, "Expenditure of operating funds to maintain existing IT-21 non-compliant NOS and applications shall be the absolute minimum necessary to meet operating requirements until IT-21 NOS/software is installed even if temporary LAN degradation occurs." (IT-21, 1997) Furthermore, applications that have typically resided on Unix platforms like JMCIS, NSIPS, TAMPS, and GCSS are now required to be DII COE compliant and should provide PC workstation access to their information over the enterprise Local Area Network (LAN).

The main proponent and change agent of the IT-21 policy is Admiral Archie R. Clemins. He explained several aspects of this policy in January 1997 when he briefed the attendees of the AFCEA West Conference in San Diego, California. Admiral Archie R. Clemins stated that the goal of IT-21 is to "...enable voice, video and data transmissions from a single desktop PC...enabling the warfighter to exchange classified and unclassified, tactical and non-tactical information." (AFCEA, 1997) To meet this goal he introduced the "Seven Habits of a Highly Effective Fleet Information Technology System." He stated that these fundamental precepts must be followed in order to guarantee the success of the Navy's information technology systems. These habits are listed below.

The Seven Habits of a Highly Effective Information Technology System

- If the Boss doesn't use it, don't buy it!
- Tactical and non-tactical must be integrated
- Stay common with industry
- Drive everything to a single PC
- Use COTS – whenever feasible
- Sea/shore transitions must be seamless

- No stove pipes

He advocates the first habit, if the boss doesn't use it, don't buy it, because if the boss is not on-board with the changes, and will not use the new IT systems, then change will not occur and IT-21 simply will not work. He supports his second habit, tactical and non-tactical must be integrated, by explaining that, "We must be able to fight the ship and run the ship from a single PC-based system. If all tactical and non-tactical applications were available on a PC, we could build, maintain, and operate PC LAN's at a relatively low cost." (AFCEA, 1997) His third habit, staying common with industry, provides benefits of low training and troubleshooting costs coupled with the cost savings provided by exploiting the research and development that has been paid for by industry. In his fourth habit he states,

> All of our applications must be connected to a Windows NT-based PC in a client-server environment, using off-the-shelf software, such as MS Office. The only exception is in very rare cases where there is an overwhelming reason to use a high-end UNIX workstation. But these uses are very rare...and becoming more rare each day. And it will give us the advantages of multiple functions on a single workstation, resulting in cost savings because work stations are cheaper, fewer workstations are required, less shipboard space is consumed...and because it assists in forcing the merging of tactical and non-tactical applications. (AFCEA, 1997)

In his fifth habit, he supports using commercial off-the-shelf (COTS) products for almost everything the Navy does. He said the Navy should treat computers as consumables vice plant property. "Life Cycle Support is neither desired nor necessary." (AFCEA, 1997) He also advocates pushing most everything the Navy does to the use of browser technology with the TCP/IP protocol. In his sixth habit, sea/shore transitions must be seamless; he advocates an architecture that provides continuous connectivity that is transparent to the end-user, whether the ship is in port or sailing the high seas. In his seventh and final habit, no stovepipes, he said there are hundreds of stovepipe systems

throughout all the military services, which burdens end-users and technicians, and prevents the Navy from staying on the cutting edge of technology. In closing he said,

> Every Sailor, Marine, Soldier, Airman and civilian in our armed forces must get on board with IT-21 in order for it to work...Eliminating stovepipes and going to a single system will pay tremendous dividends for all. It provides us the means to use fewer people to accomplish more. In short, information technology provides us with an enormous force multiplier. (AFCEA, 1997)

C. INFORMATION TECHNOLOGY STANDARDS GUIDANCE (ITSG)

In 1996, the Clinger-Cohen Act was passed which required the Department of the Navy, Chief Information Officer (DON CIO) to "develop, maintain, and facilitate the implementation of a sound and integrated enterprise architecture and standards." To comply with this law and provide a focus for the Navy standardization policy, the Secretary of the Navy "mandated that the DON CIO IPTs be the only authorized entities in the Department to develop enterprise IM/IT architecture and standards. All existing or similar efforts in the DON will be consolidated, aligned, or disestablished in order to provide the required focus and effectiveness of the DON CIO efforts." (ITSG, 1998) In order to promulgate the standards and IT architecture developed by the DON CIO IPTs, the Information Technology Standards Guidance (ITSG) was developed. The first public release of the ITSG came in June of 1998. The standards contained in the document were based on the following criteria: (1) security, (2) functionality, (3) interoperability, (4) performance, and (5) business issues.

> ***Security*** – Selected standards must support the ability to provide both system and information security.
>
> ***Functionality*** – Standards and guidance must support the fundamental requirement to ensure that IM/IT systems effectively and efficiently support the operational mission/requirements.
>
> ***Interoperability*** – applications and computers from different suppliers will have the capability to work together on a network and to connect and

share data and processes as appropriate. The model that the standards in this document follow is one that allows end systems to attach to any point on an internetwork. (End systems include clients, servers, and sensors that produce or utilize information.)

Performance – The degree of quality that a particular standard or guidance provides in selecting IM/IT products or services.

Business – Implementation cost and market acceptance of the standard or guidance is also a selection factor. Market acceptance is judged more on market momentum than on current market share. A dominant product may actually be losing market share, while an emerging product or standard may be rapidly increasing its share. By including market acceptance as one of the selection criteria, we obtain a balance in theoretical versus practical value as based on the market conclusions regarding technology, functionality and value. (ITSG, 1998)

In establishing standards, the ITSG recommends using open system standards as the preferred choice. However, a common theme of the Naval Virtual Internet document, IT-21, and the ITSG is that the Navy and Marine Corps will not accept multiple, non-interoperable products that perform a common function. In addition, "A single product suite or single product that tightly integrates multiple functions well is preferred over a federation of products, assuming there is an associated improvement in performance or price and guaranteed compliance with future open system management standards." (ITSG, 1998)

D. STAGES OF INFORMATION TECHNOLOGY TRANSITION

Before beginning a discussion of the IT-21 policy, it is appropriate to look at the position the United States Navy holds in the phases of Information Technology Transition. The Gartner Group has researched and categorized the different elements, or stages, involved in the transition of information technology in organizations. These stages are detailed below:

Stage 1: Legacy - Computing and management are centralized and hierarchical. IS organizations are in control.

Stage 2: Proliferation - IT becomes a bottleneck to progress. Technology proliferates as users independently buy their own hardware and software.

Stage 3: Interoperability - Architectures are begun with a focus on interoperability. The emphasis is on technology that is connected but unmanaged. Redundant technology costs escalate out of control.

Stage 4: Integration - Architecture and governance models emerge, multi-protocol networks are consolidated, distributed servers are deployed, data warehouses are implemented, and management of distributed data emerges. Technology costs stabilize but labor costs soar. Total-cost-of-ownership models replace traditional cost/benefit methodologies.

Stage 5: Inter-/Intraenterprise Computing - The first hints of stability emerge. A new computing and management model that supports distributed, *heterogeneous* technology and shared management of IT is extended across the enterprise and to other enterprises. Architecture and governance models are well understood, complexity is well managed, costs stabilize, and users voluntarily align with the IT strategy. (Hess and Redman, 1998)

Before Admiral Archie R. Clemins took charge to stem the tide of information systems run amuck, it is the author's opinion that the Navy was hovering between Stage 2, "Technology proliferates as users independently buy their own hardware and software," and Stage 3, "Architectures are begun with a focus on interoperability." (Hess and Redman, 1998) Now, it appears that the United States Navy is somewhere between stages three and four. In the author's opinion, the goal of the United States Navy should be to achieve Stage 5: Inter-Intraenterprise Computing.

There are likely to be several hurdles the Navy will navigate along its journey to the Fifth Stage of Information Technology Transition. A critical examination of the IT-21 policy should help to identify areas of concern or deficiencies in the Navy's current policy that can then be acted upon to help develop an improved information system

architecture. The following chapters attempt to describe what the author believes are the main deficiencies or concerns with the IT-21 vendor-based computing standard. These deficiencies will provide the threads of the argument for alternative technologies that might prove to better suite the Navy's computing needs as a matter of both function and cost. It is hoped that the ideas and alternative technologies presented in this thesis will help propel the Navy into Inter-/Intraenterprise Computing where "Architecture and governance models are well understood, complexity is well managed, cost stabilize, and users voluntarily align with the IT strategy." (Hess and Redman, 1998)

III. THE ECONOMICS OF IT-21

A. INTRODUCTION

In a discussion with University of Washington Business School students aired on the Public Broadcasting Service (PBS), Bill Gates of Microsoft Corporation spoke about the risk associated with the rapidly changing information technology market. He described how IBM had been the "king of the hill" in the information technology (IT) market, but they made some unfortunate turns at critical forks in the road. Gates was not insinuating that IBM made uninformed decisions, but he was trying to point out that IBM's decisions put them on a road that was not in concert with the market—even though IBM thought the market was going in their direction. IBM picked one direction at the fork and the market the other, resulting in huge financial losses and reduction of market share.

Microsoft Corporation is not immune to losing its dominance in a similar manner. Gates even admitted that Microsoft had been slow to realize the potential of the Internet. When Microsoft missed this path, Gates said the company went into crisis mode to try to get the company back on track with the market. They did a good job with the recovery but did have a few flops along the way. Gates went further to add that any company in the IT field can choose the wrong path and lose out on the revenue and market share that they would have otherwise dominated, making the IT market very unpredictable. With this variability in the IT market comes uncertainty and ultimately risk for consumers tasked with choosing information system standards.

Given this uncertainty and the choices made in the IT-21 policy, one might well ask, will the Navy choose the right standard? Does the Navy even need to pick such a standard? The *Information Technology Standards Guidance (ITSG)* (1998) states that "In the Naval environment, it is unrealistic to expect all platforms and activities to use a 'one

size fits all' set of standards...." However, the Navy has already adopted a vendor-based "one size fits all" standard which has its own set of risks and economic implications.

This chapter focuses on the economic impact of using a homogeneous vendor-based standard as the Navy computing architecture. It will detail the costs associated with vendor lock-in and discuss the concept or idea of "switching costs." In addition, it will demonstrate how the Navy could end up spending much more than anticipated on this standard. The hidden costs of the single vendor standard, and more specifically the hidden costs of Windows NT, will be examined. Next, a review of total cost of ownership (TCO) principles will be conducted, and the TCO of IT-21 will be explored. Finally, this chapter will examine the specific software products required by the IT-21 policy and offer some lower cost alternatives, comparable in integration ability, functionality, and ease of use. Through the examination of the concerns associated with a vendor-based standard, it is the author's belief that the Navy will be able to prevent some of the additional costs associated with that standard from rearing their head in the next generation of the Navy computing architecture.

B. SWITCHING COSTS AND VENDOR LOCK-IN

The first concern the author has with the homogeneous vendor-based standard is the increased costs the vendor can charge the United States Navy due to such factors as "switching costs" and vendor lock-in. When the Navy established its vendor-based standard, it began to make significant *durable investments in complementary assets* that were specific to that brand of computer and vendor. (Shapiro and Varian, 1999) These assets include the computer software and hardware, as well as the information, databases, and training that is produced from, or required for, the use of those systems. These "durable complementary assets" are specific to the vendor or computer platform and are mostly incompatible with alternative technologies. "These investments...," as Shapiro and Varian (1999) state, "...have differing economic lifetimes, so there's no easy time to

start using a new, incompatible system. As a result, you face *switching costs*, which can effectively lock you into your current system or brand. When the costs of switching from one brand of technology to another are substantial, users face *lock-in.*" (Shapiro and Varian, 1999)

1. Switching costs

In more basic terms, switching costs are those costs that are required to switch from one technology to another. Shapiro and Varian (1999) state that the total cost of switching to a new technology is equal to the cost the customer must bear to make the switch to the new technology, plus the cost the new supplier bears in attracting the customer away from the incumbent technology. In the information technology arena, these costs can be substantial. These switching costs can also be translated into increased profits for the supplier or increased costs for the consumer—the United States Navy. As a general rule of thumb, Shapiro and Varian (1999) state, "...the profits a supplier can expect to earn from a customer are equal to the total switching costs, as just defined, plus the value of other competitive advantages the supplier enjoys by virtue of having a superior product or lower costs than its rivals." These other competitive advantages can be real or perceived. Shapiro and Varian (1999) also claim that in general, in a highly competitive market, where the costs and quality of products are relatively the same, "...the profits that you can earn from a customer—on a going-forward, present-value basis—*exactly equal the total switching costs.*" (Shapiro and Varian, 1999)

Therefore, as the supplier of the Navy's vendor-based standard, Microsoft could increase prices to the point where the "switching costs" the Navy would have to pay to change to a new vendor's software were less than or equal to continuing to purchase Microsoft products. At this point, the Navy could decide to buy the product from another vendor and reap the benefits of the lower prices offered by the new vendor. However in the author's opinion, when a standard is set on one vendor, that vendor has "locked-in"

the military to current prices plus those additional "switching costs." This vendor "lock-in" paralyzes the Navy and causes more funds to flow from its limited coffers than would be required without such lock-in.

2. Lock-in

As switching costs "...measure the extent of a customer's lock-in to a given supplier," these two ideas are inextricable attached. (Shapiro and Varian, 1999) To gain a better understanding of lock-in, the following is provided as explanation.

> Lock-in arises whenever users invest in multiple complementary and durable assets specific to a particular information technology system. [For example] You purchased a library of LPs as well as a turntable. So long as these assets were valuable—the albums were not too scratched and the turntable still worked—you had less reason to buy a CD player and start buying expensive CDs. More generally, in replacing an old system with a new, incompatible one, you may find it necessary to swap out or duplicate *all* the components in your system. These components typically include a range of assets: data files (LP records, COBOL programs, work processing documents, etc.), various pieces of durable hardware, and training, or human capital. (Shapiro and Varian, 1999)

So at a basic level, lock-in occurs when it becomes increasingly more expensive to switch to a new technology. As described above, the more components the Navy has to switch out to change to a new vendor, the higher the switching costs and the tighter the lock-in enjoyed by the vendor. The vendor attempts to increase the switching costs in order to provide a strong lock-in, while the consumer should attempt to limit these switching costs. There are many ways in which the vendor attempts to accomplish this task. The various types of lock-in and associated switching costs are detailed in Table 3.1 below.

Table 3.1: Types of Lock-In and Associated Switching Costs

Type of Lock-In	Switching Costs
Contractual Commitments	Compensatory or liquidated damages
Durable Purchases	Replacement of equipment; tends to decline as the durable ages
Brand-Specific Training	Learning a new system, both direct costs and lost productivity; tends to rise over time
Information And Databases	Converting data to new format; tends to rise over time as collection grows
Specialized Suppliers	Funding of new supplier; may rise over time if capabilities are hard to find/maintain
Search Costs	Combined buyer and seller search costs; includes learning about quality of alternatives
Loyalty Programs	Any lost benefits from incumbent suppler, plus possible need to rebuild cumulative use

From Shapiro and Varian, 1999.

In the author's opinion, there are two main types of Lock-in that a vendor-based standard suffers: (1) brand-specific training, and (2) information and databases. These types of lock-in can be insidious, as the switching costs tend to rise over time, further solidifying the lock-in. With brand specific training,

> ...The training costs associated with replicating one's proficiency with a familiar piece of software tend to grow the more experience one has with the familiar program. Moreover, the software vendor can maintain high switching costs by introducing a series of upgrades that offer enhanced capabilities in return for the investment of additional time learning the new features. (Shapiro and Varian, 1999)

With information and databases lock-in, "...switching costs tend to rise with time as more and more information comes to reside in the historical database." (Shapiro and Varian, 1999) Both of these types of lock-in occur at the time a specific brand or vendor standard is chosen. These types of lock-in also tend to strengthen or solidify the selection

of the standard. There are several things the Navy can do to try to reduce or neutralize the amount of lock-in it has with future versions of its information system architecture.

3. Neutralizing Lock-in

Since the vendor will be trying to employ as many lock-in tactics as possible, in the author's opinion, it is incumbent upon the Navy to recognize these tactics and attempt to neutralize them. Shapiro and Varian (1999) detail the following strategies for buyers to shield themselves from some of the effects of lock-in.

- Bargain hard before you are locked in for concessions in exchange for putting yourself in a vulnerable position.
- Pursue strategies like second sourcing and open systems to minimize the extent of your lock-in.
- Look ahead to the next time you'll be picking a vendor, and take steps at the outset to improve your bargaining position at that time. (Shapiro and Varian, 1999)

Some of these concessions can come in the form of initial discounts, support in switching from another vendors software, extended service and support contracts, free upgrade, etc., and are often called "sweeteners." However, "Whatever concessions you seek, your bargaining position will be weaker once you make sunk, supplier-specific investments." (Shapiro and Varian, 1999) In the second strategy listed above, the Navy could establish two vendors, and insist that their products maintain standardized formats and interfaces. Finally, "The truly clever buyer initially leads her supplier to believe her switching costs will be large, thereby extracting a big sweetener. Later, she establishes that her switching costs are in fact much smaller, which helps her to avoid any monopolistic charges later in the lock-in cycle." (Shapiro and Varian, 1999)

C. HIDDEN COSTS OF IT-21

Now that some of the concerns with switching costs and vendor lock-in have been explored, it is appropriate to examine some other hidden costs associated with the selection of Microsoft as the IT-21 vendor-based standard. By having an understanding of what these hidden costs are, it is the author's opinion that the Navy can use that information to develop strategies to reduce or eliminate these types of hidden costs in the next information system architecture beyond IT-21. These costs are hidden in the implementation, upgrade, licensing, and support of that standard. The specifics of these costs are detailed in the paragraphs that follow.

1. Implementation Costs

One of the first hidden costs the Navy could potentially encounter is found during the implementation of Windows NT. Gartner Group analyst Weiss, in his article *Windows NT Conference Survey Results* (1997) states that despite its, "...commodity pricing and low-cost architecture...Gartner Group has found that many enterprises underestimate the amount of funding needed to execute a multiserver NT deployment." As the reader will note in Table 3.2 below, at least 90 percent of these multi-server NT deployments went over budget.

Table 3.2: Multi-server NT Deployments That Are Over Budget

Percentage Exceeded	Percentage of Enterprises
0% - 20%	10%
20% - 40%	15%
40% - 60%	20%
60% - 80%	30%
80% - 100%	15%
More than 100%	10%

From Weiss, 1997.

Not only have most of these organizations gone over budget, but they have also gone over budget by significant numbers. Fifty-Five percent of these organizations have exceeded their budget by at least 60 percent. If these figures were applied to the Navy, that means for every 100 dollars budgeted, the Navy would have to spend 60 additional unplanned or unbudgeted dollars. When zeros are added to these numbers to bring them in line with the volume of Windows NT deployments that the United States Navy will undertake, the additional unplanned—and likely unbudgeted costs—begin to accumulate rapidly. In the author's opinion, the Navy should include these budgetary "cushion factors" to allow for the deployment of Windows NT. Hopefully, the Navy can learn why these deployments went over budget and try to prevent these cost overruns in the future.

2. Upgrade Costs

Another concern with the IT-21 vendor-based standard is that of upgrade costs. Gartner Group analysts Barkan and MacDonald (1998) estimate that, "Through 2002, larger enterprises should budget for an additional 35 percent for new Windows 2000 server deployments as compared to NTS v.4...." In the author's opinion, when making information technology acquisition policy, and especially policy that calls for a single vendor standard, the cost of future versions should also be taken into consideration. As Mr. Kusnetzky, an analyst for IDC explains,

> ...Win 95 desktops will need more memory and more processing power and it's...easier to bring in a new PC than...tinker with the old one. "It could be $2,000 to $3,000 just to replace the hardware for a fairly heavily loaded system," he said. "And when you figure in the staff time it takes to move the old applications and data off the old system and onto the new, you're looking at $4,000 to $5,000." (Gaudin, 1999)

These hardware costs are only some of the costs associated with the migration to Windows 2000. The estimated software prices for the Windows NT 4.0 follow-on,

Windows 2000, are also substantial. These estimated cost increases are reflected in Table 3.3 below.

Table 3.3: Estimated Windows 2000 Retail Prices in U.S. Dollars (New Licenses)

	Current NT v4.0 List Price	NT v.4 Product	Estimated Win 2000 Price	Win 2000 Product
Workstation	$269	Workstation	$296	Professional
1-2 Processor Server	$809	Base	$890	W2S
3-4 Processor Server	$809	Base	$2,499	WAS
5-8 Processor Server	$3,999	EE	$6,999	WDCS
9-16 Processor Server	OEM Only	OEM Only	$6,999	WDCS
16+ Processor Server	N/A	N/A	OEM Only	OEM Only

*Estimates are based on list prices. Percentage differentials will approximate Microsoft Select percentage price changes. Organizations should determine the percentage changes in their own contract pricing and apply this to their anticipated mix of one- to eight-way processor servers to determine the overall price impact, which may be more or less than these projections.

W2S - Windows 2000 Server

WDCS - Windows 2000 Data Center Server

WAS - Windows 2000 Advanced Server

EE - Enterprise Edition

From Barkan and MacDonald, 1998.

While Workstation and One-to-Two Processor Server price increases are relatively low (nine plus percent for both), the price increases for more than two processor servers can be as high as 309 percent. As is evident in the table above and in the previous discussion, these price increases are going to put a serious dent into the Navy's IT funding pockets if the Navy has not budgeted for this additional nine to 309 percent to upgrade to the next version of the Windows operating system.

With every new version of an Operating System, there are likely to be improvements and added functionality that might warrant an increase in the price for that product. Windows 2000 is advertised to provide a number of significant functional changes, but as Gartner Group analysts Barkan and MacDonald (1998) point out:

> Microsoft's naming change should not be confused with a technology change. We believe Microsoft changed the name to create an opportunity

> for further tiering of server products to raise server OS prices, which also enables Microsoft to realign the packaging of its BackOffice products to raise BackOffice prices, and to create the illusion for its enterprise Windows 95/98 installed base that Windows 2000 is the logical upgrade path in an attempt to convince business users to move to the higher-priced Windows 2000 from Windows 95/98. (Barkan and MacDonald, 1998)

In the author's opinion, when the Navy established its vendor-based standard, it also created a level of lock-in to future versions of the operating system and office automation system software. As a result, it became somewhat tied to the vendor and the additional costs associated with upgrading to the next version of that vendor's software. When establishing the standardization policy after IT-21, the author believes the Navy should use these added lock-in costs as leverage to get more favorable licensing terms, or to try to neutralize or minimize the lock-in altogether.

3. Licensing Costs

Another concern the author has identified with the current standard is the hidden licensing costs the Navy might be experiencing. One technique that Microsoft has used to increase prices is to alter the Terms and Conditions (T&C's) of its licensing agreements. Most software vendors have a clause in their licensing agreements that allows them to change the T&C's with, or without, a warning period (usually 30 days). Most of these changes have been seen in the restriction of usage rights. While this might seem benign on its face, these changes in T&C's can be costly. While no change in desktop price has been made, Microsoft has been subtly increasing costs through altering the T&C's of their licensing agreements. As Gartner Group Analyst Bona (1998) describes:

> Indeed, since 1996 Microsoft has not increased desktop pricing for Variable clients, but has been restricting usage rights. These changes, which at first appear to be innocuous nuances, have severe cost implications. An analysis of a typical 5,000 desktop Enterprise licensing

> Office demonstrates the dramatic financial impact. The elimination of home use, concurrent use and the proration of maintenance represent a 224 percent price increase in pricing—even though list pricing on Office has been flat. (Bona, 1998)

So what are the usage rights that are being restricted? "Home Use" is a term used to describe the process by which the primary user of the computer where the software is installed may make a second copy for use on either a home or portable computer to do work at home. "Concurrent Use" is the sharing of software licenses among many users recognizing the fact that not all users are using computer services at the same time. "Maintenance," in all practicality, means that the enterprise has to pay to run previous versions of an operating system if their computer came with a newer version of the operating system. For example, if the Navy decides *not* to convert to Windows 2000 as soon as it is released (as recommended by Gartner Group), they will have to pay maintenance on those new machines that they purchased with Windows 2000 pre-installed but on which they want to run Windows NT 4.0. The main reason for the "maintenance" requirement is that, "Microsoft OS licenses are machine specific and are tied to the serial number of the hardware. They may not be transferred to another machine. Enterprises cannot transfer a license from a machine they are replacing to a new machine to get the prior version rights," under certain licensing schemes. (Bona and Welch, 1998) The loss of these usage rights might not apply to all of Microsoft's products or licensing schemes, but with the volume of Microsoft products the United States Navy is expected to purchase, the Navy is bound to be affected by some of these changes. In the author's opinion, this could ultimately result in increased costs for the United States Navy to the tune of some 224 percent, and the Navy will never see an increase in the product's list price. It is this type of hidden cost, one that is truly hard to detect, which the Navy should try to identify and avoid.

4. Support Costs

The final hidden cost associated with the Windows NT/IT-21 standard is that of support costs. Some of these costs have increased significantly for private sector organizations. As Garvey notes in his *Information Week Online* article, *The Hidden Cost of NT* (1998), "The support costs and staffing required for the care and feeding of NT are causing some adopters to abandon NT Server as a strategic application platform—often relegating it to the task of file-and-print serving." Some enterprises that require high availability and low maintenance are finding that NT is not up to the task. Bob Cargill, Oriental Trading Company's systems manager, claims, "Once a week it [Windows NT Server] goes down—anywhere from 15 minutes to several hours before we figure out what's wrong...That's not what we want in a Web server. When customers aren't able to get through and place their orders, that's a ticket to low customer satisfaction." (Garvey, 1998) This $200 million dollar direct marketer can not stay in business with the excessive downtime and high maintenance demands of Windows NT. As a result, Oriental Trading Company said it planned to move its Internet server off Windows NT Server. (Garvey, 1998)

There are even those that are finding that Windows NT is not as competitive with routine file-and-print requirements. Aberdeen Group's analyst Sachikiny says, "A client recently evaluated replacing Novell NetWare with NT. But when company officials realized they would need five NT servers for every three NetWare servers, they decided to keep their Novell network." (Garvey, 1998) In the author's opinion, NT Server is not always competitive with other technologies and the United States Navy should exercise greater caution when deciding to purchase all of its operating system and computer applications from a single vendor.

Gartner Group analyst Thompson notes in *Justifying Windows NT: Too Much Monkey Business (1998),* "A 'pure NT' environment will save less than 10 percent of a

TCO compared with a mixed [Windows NT-Windows 95/98] platform environment." In the author's opinion, it seems as if the Navy has the false goal of having 100 percent compliance with the standard rather than focusing on the true goal of interoperability and reduced cost. If the Navy continues down the path of creating a purely homogeneous vendor-based information system standard, the Navy will most likely fail. As the Gartner Group notes,

> Through year-end 2000, 90 percent of all organizations attempting a 100 percent pure Windows NT migration at the desktop and mobile level will fail...An NT migration can be used as a catalyst to help reduce the degree of variance in both OSs and applications. However, managed diversity according to user need is, in most cases, cheaper than trying to build a homogeneous environment. (Thompson, 1998)

These odds are not in favor of the United States Navy. In the author's opinion, it seems as if the Navy is trying to throw technology (a single operating system/single PC standard) at a management problem. The Navy should concentrate on strictly managing a heterogeneous computing environment if it expects to achieve its goals of interoperability and reduced computing costs. The Navy must solve its management problem with—good management.

D. TOTAL COST OF OWNERSHIP (TCO)

Total Cost of Ownership (TCO) is a term that has been around for some time and it has captured the attention of many a senior level manager. These managers understand the benefit of using TCO analysis to support their information technology acquisition decision-making policies, but due to the complexities and cost of the analysis, it is often not performed. In fact, as Aberdeen Group (1999) notes after studying the practical application of TCO analysis,

> If an IS manager is asked 'Is TCO important to you when you are choosing an application server?' the majority of respondents will answer yes. However, if an IS manager is asked 'Did you do a TCO analysis to

choose your application server?' all will answer no. (AberdeenGroup, 1999)

The problem confronting corporate organizations and the United States Navy is that these analysis are hard to perform, and it is hard to get the data, or measure data, for these analysis. As a result, these analyses are often incomplete or not performed at all. While it is difficult to perform such an analysis, it is the author's belief that it is still important to do as much of a TCO analysis as possible to help determine most, if not all, the costs associated with its IT investments. In order to perform a Total Cost of Ownership analysis, one must have a good TCO model.

1. Gartner Group TCO Model

As Interpose, Inc. (1997) explains, "The objective of any TCO analysis is to maintain or maximize individual productivity while lowering costs." (Interpose, 1997) At its very basic level, a TCO model is used to help organizations determine and understand the direct (budgeted) and indirect (unbudgeted) costs associated with owning, using, and managing a particular IT investment throughout its lifecycle. A combination of a TCO model and management philosophy provides an organization with a greater understanding of all the costs associated with their distributed computing infrastructure and can be used as a decision support tool. Most TCO models divide costs into categories that allow costs between organizations to be simulated and analyzed in a detailed, reliable, and consistent manner. In the author's opinion, this can help the Navy determine how to better manage its current investments and how to reap greater value from new IT investments. No one TCO model is any better than any other model. As long as the same model is used in comparing different alternatives, and all relevant costs are accounted for in the model, it should help in making unbiased comparisons.

The Gartner Group TCO Model utilizes two major categories to organize costs, direct (budgeted) costs and indirect (unbudgeted) costs. These costs are described in the paragraphs that follow.

Direct (Budgeted) Costs - measures the direct expenditures on IS by an organization (capital, labor, and fees).

Hardware and Software – the capital expenditures and lease fees for servers, client computers (desktops and mobile computers), peripherals, and the network.
Management – the direct network, system, and storage management labor staffing, activity hours and activity costs and the professional services outsourcing fees.
Support – the help desk labor hours and costs, help desk performance metrics, training labor and fees, procurement, travel, maintenance/support contracts, and overhead labor.
Development – the application design, development, test, and documentation including new application development, customization, and maintenance.
Communications Fees – the inter-computer communication expenses for lease lines, server access remote access, and allocated WAN expenses.

Indirect (Unbudgeted) Costs - measures the capital and management efficiency of IS in delivering expected services to end-users.

End User IS - the cost of end users supporting themselves and each other instead of relying on formal IS support channels (peer and self support), end user formal training, casual learning (non-formal training), and self-development/scripting of applications.
Downtime – the lost productivity due to planned (scheduled) and unplanned network, system, and application unavailability, measured in terms of lost wages (lost productivity). (Gartner Group, 1998)

2. PC/LAN TCO Cost Categories

The Gartner Group has been using TCO analysis for over a decade to effectively measure the total cost of owning a variety of different platforms. Gartner Group estimates

that, "...each PC within an enterprise can carry a TCO as high as $10,000 per year." It has been the power and functionality that Microsoft has built into their products that has driven the TCO of the desktop to these high levels. (Gartenberg, 1998) While software prices have increased in many cases through the addition of this functionality, hardware prices have been on a steady decline. How do all the costs associated with an information system break down? The major cost categories of a PC/LAN Total Cost of Ownership are displayed in Figure 3.1 below.

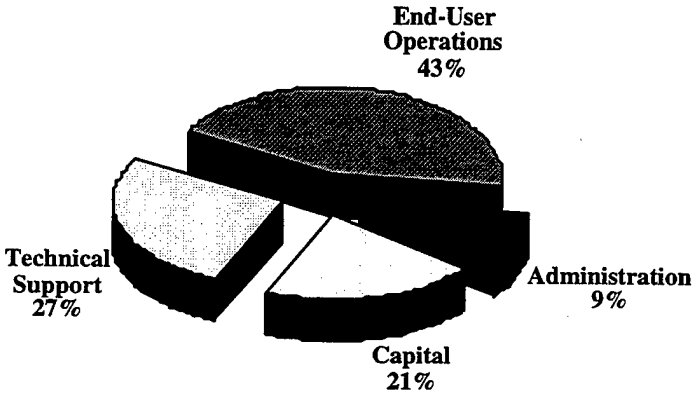

Figure 3.1: PC/LAN Total Cost of Ownership

From Cappuccio, Keyworth, and Kirwin, 1996.

While the source of the graph above is from 1996, the exact percentages are not as important as the major tendencies that these figures exhibit. As demonstrated in the figure, most of the cost of a PC attached to a LAN is absorbed by end-user operations, and this category is not a budgeted cost for most information technology organizations. Capital expenditures account for a relatively small percentage of the Total Cost of Ownership, but it is still a valid area to examine when trying to reduce costs. In the author's opinion, when looking to make cost savings, the Navy must be careful because when a reduction happens in one category, it is sometimes matched by a corresponding

increase in another category. The goal of an IT manager is to lower costs in all categories through an effective cost reduction *and* management philosophy.

E. TOTAL COST OF OWNERSHIP OF IT-21

1. IT-21 Projected Savings

While many recognize that TCO can help in the effective deployment of information technology, it is very expensive, and it is often hard to get all of the information required to calculate the intangible end-user, unbudgeted costs. Even with these difficulties, the architects of the IT-21 policy were able to conduct such an analysis. A Navy "Computing Cost Baseline" with and without IT-21, was calculated based on a 650 seat configuration. The results are enumerated in Tables 3.4 and 3.5 below.

Table 3.4: Computing Cost Baseline (without IT-21) (Basis: 650 seats)

System/Network Management Cost		User Cost	
Systems Administration -One FTE per 50 seats	$455K	User Downtime (Assumed 5% incl. upgrades)	$1,200K
Applications Management -One FTE per 100 seats	$228K	Lack of Collaboration (Assume 3% of time)	$720K
Support Desk -One FTE per 200 seats	$114K		
Network Management -One FTE per 100 seats	$228K		
Asset Management -Four manweeks per year	$3K		
Capacity Planning -Six manweeks per year	$4K		
Hardware	$619K		
Software	$130K		
Training	$884K		
Total Cost	$2,670K	Total Cost	$1,920K
Cost Per Seat	$4,100	Cost Per Seat	$2,900
Total Cost Per Seat: $7,000			

From Cebrowski, 1997.

Table 3.5: Computing Cost Baseline (with IT-21) (Basis: 650 seats)

System/Network Management Cost		User Cost	
Systems Administration	$114K	User Downtime (Assumed 1% incl. upgrades)	$240K
Applications Management	$76K	Lack of Collaboration (Assume 1% of time)	$240K
Support Desk	$35K		
Network Management	$76K		
Asset Management	$1K		
Capacity Planning	$1K		
Hardware	$608K		
Software	$47K		
Training	$663K		
Total Cost	$1,600K	Total Cost	$480K
Cost Per Seat	$2,500	Cost Per Seat	$740
Total Cost Per Seat: $3,200			

From Cebrowski, 1997.

From these tables it was stated that there would be a 70 percent reduction in software costs, 75 percent decrease in end-user technical support costs, and an 80 percent decrease in overall PC and user support costs with the adoption of the IT-21 vendor-based standard. It was also stated that new PC installation times were reduced from a day to less than one hour. (Cebrowski, 1997) However, in the author's opinion, some of the numbers made assumptions that were not in concert with real-world data.

a. Adjusting Cost Baseline to Accommodate Real-World Data

To begin, the assumption for user downtime with IT-21 is inaccurate. Using data from Gartner Group studies, Windows NT has an average availability of 97.44 percent, which equates to 224.5 hours of downtime per year. (Fitzpatrick, 1998) This figure is buttressed by additional real world Navy data. As Bryan Scurry, a test

director for the Space and Naval Warfare Systems Command (SPAWAR), affirms during a test of the NT-based Global Command and Control System-Maritime (GCCS-M), the system ran "for more than 1,000 hours, and it passed with an operational availability of over 95 percent. In a couple of instances, the availability hit 98 percent." (Brewin, 1998) This real-world data would cause an increase in the assumed downtime of one percent with IT-21, to a more realistic three percent.

In staying under the general heading of "User Cost," there is no accounting of "Hey Shipmate" costs, or the cost of end users supporting themselves and each other, instead of relying on formal IS support channels. This type of cost is dangerous because it is hard to quantify and it is often not budgeted. If more people exercise "Hey Shipmate" solutions instead of using the "help desk," then the statistics for use of the help desk will decrease. These statistics can then be used to justify a reduction in the help desk staff, which in turn causes more "Hey Shipmate" solutions. In the author's opinion, this spiral causes a shift in IT costs from the budgeted category to the unbudgeted category, and puts the Navy in a position where they do no know what they are paying for their computing needs. With the move to a homogeneous vendor-based Windows NT standard, the author believes the Navy needs to ensure they do not skimp on the staffing of the administration and support of those systems simply because they are supposed to be easy to use. As Gartner Group analyst Silver explains, "Enterprises that skimp on staffing NT projects by 20 percent to 50 percent will incur 50 percent to 100 percent higher TCO than those that are properly staffed." (Silver, 1998) To account for these "Hey Shipmate" costs, the "Lack of Collaboration" for IT-21 will be increased one percent.

Now that end-user costs have been adjusted closer to real-world data, in the author's opinion, it is now time to examine the System and Network Management costs. Using the logic of the calculations in Tables 3.4 and 3.5, the Computing Cost

Baseline without IT-21 would require 30 Full Time Equivalent (FTE) employees to administer the 650 seats, and the Baseline with IT-21 would require nine FTEs. However, the IT-21 policy did not name any management software or management policies to help these remaining administrators operate at these reduced manning levels. As a result, the author questions whether or not these reductions can be successfully accomplished. As Gartner Group analyst Gartenberg explains,

> Lower TCO is often confused with the enabling technologies that can help implement best practices. While enabling technologies like Zero Administration Windows and such concepts as network computing can serve as the technology architectures that lead to lower TCO, it is the implementation of these tools coupled with a management philosophy of central administration that delivers the lower costs. In fact, mistaken belief that technology is the answer to lower TCO can often increase costs. For example, Windows NT version 4.0 delivers a lower TCO than Windows 95, but only when implemented with a management philosophy and using such key features as policies and administration. (Gartenberg "Beyond", 1998)

The IT-21 Baseline states that only one FTE is required for the "Support Desk." One FTE works 2,080 hours per year. This represents eight-hour days with five-day weeks. The military does not work on such a liberal time schedule. In fact, the Navy often requires that its information systems be operational 24 hours a day, seven days a week. If the Navy is becoming more reliant on IT, the author believes the Navy will probably be required to provide support for their information systems on that schedule also. There are 8,736 hours in a year. To accommodate 24-hour operations, the support desk would have to be staffed with a minimum of three FTE to allow for the 24-hour operations, sicknesses, and personal leave for IT staff.

The final area of the System and Network Management Costs that will be explored is that of software costs. From Tables 3.4 and 3.5 it was claimed that there was a 70 percent reduction in software costs. If one does the actual calculation, a 64 percent

reduction of the $130,000 cost of software without IT-21 would yield the $47,000 cost claimed with IT-21 vice the 70 percent stated.

Furthermore, it is helpful to look at what that $47,000 would buy to see if it is in concert with real-world data. A $47,000 software cost based on 650 seats would yield a cost of $72.31 per seat. The retail version of Microsoft Back Office, Client Access Licenses (CAL) cost $4,179 for 20 CALs, which translates into $208.95 for one CAL. If you depreciate this over three years, as recommended by the Gartner Group, it would cost $69.65. That leaves $2.66 per seat per year to buy Microsoft Windows NT Workstation, Microsoft Office Professional 97, and Norton Anti-Virus. Volume licensing should reduce this figure somewhat, but in the author's opinion, it is unlikely that the Navy can reduce the software costs to this level. In addition, the hidden costs associated with licensing, upgrades, and implementation, make this number unrealistic.

In an attempt to introduce more real-world data into the savings that an IT-21 vendor-based standard could provide, the author offers Table 3.6 for comparison. These figures were calculated using the logic of Tables 3.4 and 3.5, and continue to represent an estimate of the cost savings.

Table 3.6: Computing Cost Baseline/Real World Data (with IT-21)

(Basis: 650 seats)

System/Network Management Cost		User Cost	
Systems Administration -One FTE per 130 seats	$175K	User Downtime (Assumed 3% incl. upgrades)	$720K
Applications Management -One FTE per 217 seats	$105K	Lack of Collaboration (Assume 2% of time)	$480K
Support Desk -One FTE per 217 seats	$105K		
Network Management -One FTE per 217 seats	$105K		
Asset Management -Four manweeks per year	$1K		
Capacity Planning -Six manweeks per year	$1K		
Hardware	$608K		
Software	$100K		
Training	$663K		
Total Cost	$1,863K	Total Cost	$1,200K
Cost Per Seat	$2,866	Cost Per Seat	$1,846
Total Cost Per Seat: $4,712			

After Cebrowski, 1997.

Herein lies the problem with conducting a Total Cost of Ownership analysis. Since, the Navy does not have all the information required to make such an analysis, and the author does not have all of the information required to make such an analysis, some items must be estimated. In this case, the Navy has underestimated the costs required to implement this vendor-based standard in the author's opinion.

Performing a complete TCO analysis is also beyond the scope of this thesis, but this section will attempt to establish assumptions that will freeze all costs except capital costs in an effort to illustrate the cost savings that could be achieved with other standards. Specifically, the analysis of capital costs, which are easier to quantify,

will demonstrate the savings that can be achieved through the use of Open Source Software.

2. Economic Alternatives to the Single Vendor Standard

Three examples will be examined to determine the capital costs of: (1) the homogeneous IT-21 vendor-based standard, (2) a heterogeneous mix of vendor-proprietary and open source software, and (3) a homogeneous open source software standard.

In these examples, it will be assumed that the hardware required for each alternative is equivalent, even though Windows NT would require hardware upgrades in some cases. In each example, an organization will be established that requires a file and print server, a web server, and a mail server—not unlike many organizations in the United States Navy. This organization will have 100 members in an attempt to make it easier to scale the outcome to a larger number of users.

The *Information Technology for the 21st Century* message provides the following as a list of standard software to be used in the fleet.

IT-21 software:

- Microsoft Windows NT 4.0/5.0 Workstation
- Microsoft Office 97 Pro (Word 97, PowerPoint 97, Excel 97, Access 97)
- IBM Anti Virus (Navy License, available from NAVCIRT)
- Microsoft Back Office Client
- Microsoft Outlook 97
- Microsoft Exchange 5.0
- Microsoft Image Composer

Some of this software is no longer available in the same form as described. The differences made to the examples that follow will be explained to match them as closely as possible to the standards above.

a. IT-21 Homogeneous Vendor-Based Standard

In the first example, the cost of using the IT-21 vendor specific standard will be calculated to set a baseline for further comparison. Microsoft Outlook 97 is now part of Microsoft Office Professional 97 so there is no extra charge for Outlook 97. Microsoft Image Composer is no longer sold as an individual product; it is part of Microsoft FrontPage 98. As a result, one copy of FrontPage 98 is substituted for Image Composer assuming only one copy will be required in the command. IBM Anti-Virus no longer exists as is named. On May 19, 1998, IBM and Symantec combined resources to produce one family of anti-virus software products—Norton Anti-Virus. Therefore, Norton Anti-Virus is substituted for IBM Anti-Virus and the price reflects the cost of Norton Anti-Virus. These costs also assume that no machines originally came with Windows NT Workstation pre-installed. Furthermore, Microsoft Exchange 5.0 is now Microsoft Exchange 5.5, so the new version prices will be used in the example. These are the minimum software costs associated with the IT-21 vendor-specific standard if purchased *without* volume licensing. These results, as well as the results in the subsequent examples, would be smaller with volume licensing schemes. However, since all examples will use the vendor's list prices, the author believes this should result in a fair comparison of alternatives. The details of these costs are enumerated in Table 3.7 below.

Table 3.7: IT-21 Homogeneous Vendor-Based Standard

Product	Price per Unit	100 User Price
Microsoft Office Pro 97 - Microsoft Outlook 97	$569.00	$56,900.00
Microsoft FrontPage 98 - MS Image composer	$109.00	$109.00
Norton Anti-Virus 5.0 (IBM Anti Virus)	$39.95	$3,995.00
Windows NT 4.0/5.0 Workstation (w/service pack)	$319.00	$31,900.00
Microsoft Back Office Client (20 Client Access Licenses)	$4,179.00	$20,895.00
Microsoft Exchange Server 5.5 w/5 Client Access Licenses (Microsoft Exchange 5.0)	$999.00	$999.00
Windows NT Server w/5 Client Access Licenses, NT Option, and Service Pack	$809.00	$1,618.00
	Total	$116,416.00

After Microsoft, 1999 and Symantec, 1999.

In the author's opinion, the mere fact that all of these substitutions were required in this example is yet another reason for not having a vendor-based standard. With the constant change in the IT industry, and given the slow pace of implementation and transition in the Navy, the vendor-based standards are out of date before they can even be implemented.

b. Heterogeneous Mix – Proprietary and Open Source Standards

In the second example, the organization would substitute the two Windows NT Servers and the Microsoft Exchange Server in the back-end of the organization with Linux Servers using Samba and Sendmail. Samba is a program that

allows Linux servers to look and act like a Windows NT Server to the client. This substitution would eliminate the need for Client Access Licenses and also provide the front-end, or user end, with the same user interfaces that they are accustomed. Sendmail will act as a Mail Transport Agent for Linux. There is even a project afoot in the Linux community to produce a program, called WINE, which will allow Windows applications to run on the Linux operating system. The heterogeneous open source alternative is detailed in Table 3.8 below.

Table 3.8: Heterogeneous Open Source/Proprietary Alternative

Product	Price per Unit	100 User Price
Microsoft Office Pro 97 - Microsoft Outlook 97	$569.00	$56,900.00
Microsoft FrontPage 98 - MS Image composer	$109.00	$109.00
IBM Anti Virus (Norton AntiVirus 5.0)	$39.95	$3,995.00
Windows NT 4.0/5.0 Workstation (w/service pack)	$319.00	$31,900.00
No Client Licenses Required	$0.00	$0.00
Red Hat Linux	$0.00	$0.00
Red Hat Linux	$49.95	$49.95
	Total	$92,953.95

After Microsoft, 1999, Red Hat,1999, and Symantec, 1999.

Since the end-user, in this example, does not have a change in software or equipment, end-user costs can be assumed to be constant or relatively constant. There would however be an increase in administration costs. The cost savings from using these Linux servers could be used to pay for these additional administration costs. The low cost of the software and the high availability of Unix/Linux compared with Windows NT, as demonstrated in Chapter V of this thesis, should provide adequate resources for the training of the system administrators.

c. *Homogeneous Open Source Standard*

In the third example, all IT-21 vendor-based software will be removed and only open source software alternatives will be used. The total cost of an open source software solution is enumerated in Table 3.9 below.

Table 3.9: Homogeneous Open Source Alternative

Product	Price per Unit	100 User Price
Applixware for Linux Deluxe - Included in Applixware	$99.00	$9,900.00
Included in Applixware - Included in Applixware	$0.00	$0.00
No Virus Software Required	$39.95	$3,995.00
Red Hat Linux	$0.00	$0.00
No Client Licenses Required	$0.00	$0.00
Red Hat Linux	$0.00	$0.00
Red Hat Linux	$49.95	$49.95
	Total	$13,944.95

After Red Hat, 1999.

In this example, Applixware for Linux Deluxe provides comparable functionality to Microsoft's Office Professional 97 and FrontPage 98. Applixware for Linux Deluxe includes Applix Words, Presents, Spreadsheets, Data, Mail, Builder, HTML Author, and Applix Graphics programs. These programs operate in a similar manner to the Microsoft Office programs and even have filters to convert to and from some of these Office programs. There are even rumors that Microsoft is pursuing the development of a version of Office for Linux, which could potentially be used in the future. In addition, there are currently no viruses for Linux. However, the author has included the price of Norton Anti-Virus version 5.0 to cover the costs of some future virus. This cost might not be needed because the open source community often produces programs and bug fixes with little to no cost, but it is included anyway, in an attempt to create a fair comparison. Finally, with Linux on the desktop, no end-user licenses are

required, and one copy of Linux provides unlimited user license. As a result, one copy of the program can be legally installed on all of the computers in the organization.

With the substitution of Linux as the desktop operating system, capital costs are significantly reduced. However, this substitution would also correspondingly increase end-user costs to some unknown amount because end-users would have to be trained on a new operating system. As demonstrated in Chapter V of this thesis, the availability of Unix, and its variants, is higher than that of Windows NT. The cost-savings resulting from this higher availability could be used to offset part of those end-user-training costs. While Linux is an up-and-coming operating system, in the author's opinion, it is not quite ready for "primetime" on the desktop. However, with a little more work on a user-friendly interface, Linux should be a viable contender to Windows NT Workstation on the desktop in the future. However, by choosing vendor-based standards, large buyers can seriously delay or prevent this from happening. Furthermore, the selection of a single vendor-based standard will prevent the Navy from using Linux, or any other operating system in the future, if they should become viable desktop computing options.

d. Analysis and Cost Comparison

To fully appreciate the magnitude of the costs in these examples, the graph in Figure 3.2 below is provided to help the reader compare the differences in software costs among alternatives.

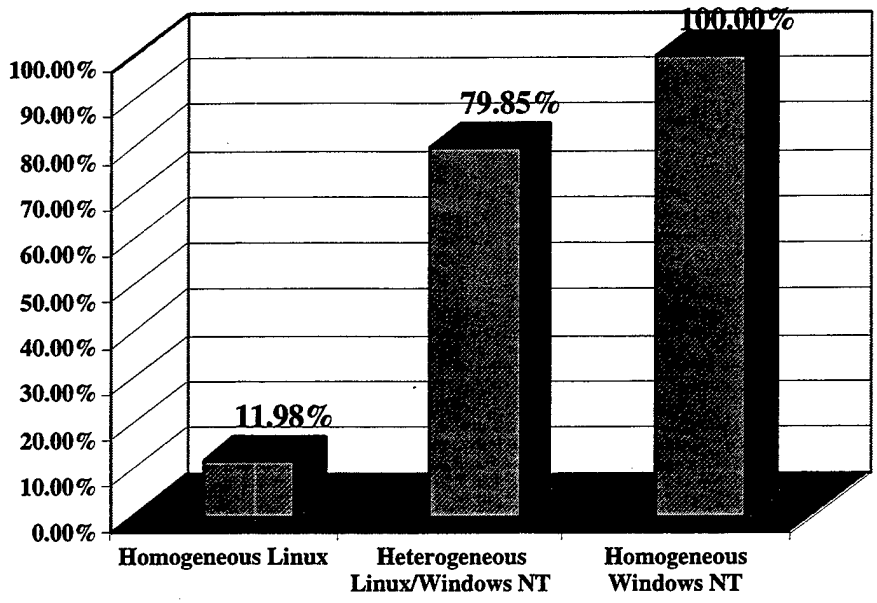

Figure 3.2: Percentage of IT-21 Software Costs

Will end-user costs be increased over $1,000 dollars for each user if the standard were changed to Linux? It is highly unlikely, but that is what would be required to make Linux an unsound economic alternative from a pure capital cost perspective. A homogeneous Linux solution would cost 11.98 percent of the currently stated IT-21 policy. The remaining 80+ percent could be used to provide training and be used as cost savings. With a mature Linux, these types of savings could soon become a reality.

When examining the homogeneous alternative to the IT-21 standard detailed above, it is apparent that from a sheer capital cost point of view, this standard could provide significantly reduced capital costs. While other homogeneous solutions provide significantly reduced costs, this thesis does not recommend a homogenous information system standard. The point the author is trying to convey is simply that from an economic point of view, a Microsoft-based standard is not necessarily the best alternative, even among the single vendor solutions.

F. LINUX

Since much has been said about Linux in this Chapter, the following is offered to give the reader a greater understanding of the Linux operating system. Linux is a form of open source software. Open source software is as much a philosophy as a category of software. "Open source promotes software reliability and quality by supporting independent peer review and rapid evolution of source code. To be certified as open source, the license of a program must guarantee the right to read, redistribute, modify, and use it freely." (Raymond, 1999) Netscape and Apple Computer are some of the more notable examples of companies that have released all or some of their source code as open source. The open source philosophy promotes increased security and greater flexibility, and the free nature of the software is nice on the bottom line of almost any organization.

Linux (pronounced lynn-ucks) is an open source operating system that had its genesis in 1991. At that time, Linus Torvalds began building the operating system as a hobby, and then that operating system blossomed into a full-featured variant of the Unix operating system. Hundreds of programmers joined in the effort and today Linux is a viable contender for the server network operating system market. With some maturity, the author believes Linux could grow to challenge the desktop operating system market dominated by Microsoft. Linux is free if downloaded from the internet, but companies like Red Hat and Caldera, among others, produce a shrink wrapped version of the software that provides an installer program and product support for around $50 dollars for unlimited user licenses.

1. A Comparison of Linux/NT/Unix

One of the main reasons given for the inclusion of Microsoft Windows NT as a standard, and the exclusion of other operating systems as a standard, is that NT excels in

the area of packaged applications. Linux is showing rapid growth in this arena. Many vendors have already ported their applications to Linux or are planning to port their applications to Linux. Netscape, Corel, and Oracle are some of the more notable companies who have already produced Linux versions of their flagship products. In May of this year, Novell announced that they were creating a native Linux version of Novell Directory Services to be released toward the end of 1999. This release "will enable customers to effectively manage Linux workstations and servers and integrate these Linux resources with NetWare, NT and Solaris systems on enterprise networks." (Merritt, 1999) As Gartner Group analyst Weiss (1998) claims, "...support for Linux by such DBMS vendors as Oracle, Informix, Sybase, and IBM will narrow this advantage [in packaged applications] over time." (Weiss, 1998)

Gartner Group compiled information displaying the differences between Linux, Windows NT version 4.0, and leading Unix platforms. Table 3.10 is provided to give the reader a better understanding of these differences.

Table 3.10: Linux/Windows NT/Commercial Unix Comparison

	Linux	Windows NT 4.0	Leading Unix*
Hardware Platforms	Many	Intel, Alpha	Narrow choices
OS Reliability and Stability	High	Medium	High
SMP Support (Realistic Range)	4-way	4-8 way	16-way
64-bit OS Support	Since 1995	Due 2000/2001	All leaders
Configurability	Medium	Medium	High
OLTP, Messaging Middleware Availability and Quality	Low	High	High
DBMS Support	Low	High	High
DBMS Scalability	Medium	Medium	High
Clustering	Special	Early stages	Good
Ease of use (expertise)	Medium	Low	High
Technical support	Limited	Medium	Deep
ISV Support	Limited	High	High
Windows Client Support	Limited	High	Medium
Quality and scope of system management tools	Low	Medium	High
Java and development Tools	Low	High	High
Software Pricing	Very low	Medium	Medium-high

*(e.g., Solaris, HP-UX)
From Weiss, 1998.

Those areas where Linux is weak, like DBMS Support, Technical Support, and ISV Support are all changing. Vendors continue to port their applications to Linux, and companies like Red Hat and Caldera continue to increase their technical support to the end user. Linux strengths are in its high reliability, stability, and software pricing.

Enterprises have seen these strengths and have been quietly deploying Linux in their networks as a cost saving, reliable alternative to Windows NT. These "Back-door opportunities for Linux have resulted from uncertainty surrounding Microsoft's ability to deliver timely improvements; OS stability, scalability and availability; and the broadening pervasiveness of Web applications." (Weiss, 1998) Burlington Coat Factory Warehouse Corp.'s, for example, plans to implement the largest Linux retail installation

announced by a United States company. "In all, the hardware will cost $1.15 million to $1.8 million, depending on the power of the machines...The cost of Linux itself...will be only a few hundred dollars. Thus, Burlington will save thousands of dollars in each store by not buying a commercial operating system." (Orenstein, 1999) In the author's opinion, this deployment shows great confidence in the Linux operating system.

The military is also using Open Source Software—they just don't advertise its use. The common claim is: "No one ever got fired for using Microsoft." However, in the author's opinion, system administrators have realized that Windows NT is not highly reliable and they have been secretly installing these low cost alternatives to help increase the reliability of their networks, and as a low cost alternative when maintenance is being conducted on their Windows NT servers. For example, before the DON CIO moved its web server to Windows Internet Information Server it used the open source server software, Apache, to serve up its web site. In addition, when the BUPERS web site was recently down for Y2K compliance maintenance, they used an Apache server to maintain access to their web site. But let's not take private enterprise or the militaries word for Linux's price/performance characteristics; let's see what Microsoft has to say about Linux.

2. The Halloween Papers

On or about Halloween 1998, two internal Microsoft Confidential documents detailing open source software and Linux were leaked to the Internet. These documents titled *Linux OS Competitive Analysis: The Next Java VM* and *Open Source Software: A (New?) Development Methodology* were prepared by Microsoft Engineers Valloppillil and Cohen, and have been affectionately dubbed the Halloween Documents. As Microsoft Engineer Valloppillil states in *Linux OS Competitive Analysis: The Next Java VM (1998),* "The primary threat Microsoft faces from Linux is against NT server." Microsoft is concerned about Linux and these concerns are buttressed by several key

strengths Linux has against NT server. As Valloppillil and Cohen explain in the Halloween documents (1998),

- Linux uses commodity PC hardware and, due to OS modularity, can be run on smaller systems than NT. Linux is frequently used for services such as DNS running on old 486's in back closets.
- Due to its UNIX heritage, Linux represents a lower switching cost for some organizations than NT.
- UNIX's perceived Scalability, Interoperability, Availability, and Manageability (SIAM) advantages over NT.
- Linux can win as long as services/protocols are commodities.
- Linux represents a best-of-breed UNIX, that is trusted in mission critical applications, and—due to it's open source code—has a long term credibility which exceeds many other competitive OS's.
- Most of the primary apps that people require when they move to Linux are already available for free. This includes web servers, POP clients, mail servers, text editors, etc.
- An advanced Win32 GUI user would have a short learning cycle to become productive [under Linux]. (Valloppillil and Cohen, 1998)

This last point could prove to be beneficial to the United States Navy. Linux, and other Unix variant operating systems, have had a graphical user interface (GUI) for years now, and Microsoft's admission that a Win32 GUI user would have a short learning cycle to become productive under Linux gives added credibility to the claim that switching to Linux would not severely impact Navy end-user costs.

Finally, as the IT-21 policy (1997) states, "The IT-21 standards...represent front end market technology, are dynamic in nature, and will continue to be closely linked to commercial trends." Commercial trends seem to be moving towards, and embracing, Linux. Hewlett Packard, Silicon Graphics, Compaq Computer, Dell, and IBM have all agreed to include Linux on some of their machines. Furthermore, Oracle, Informix, Netscape, Corel, and others have already ported their applications to Linux. Linux is also gaining an ever-increasing share of the server operating system market. As Market Research Company IDC reported late last year,

> ...Throughout 1998 Linux's share of the server operating system market grew 212 percent, leaving Linux with 17.2 percent of the market, up from 6.8 percent in 1997. Windows NT led the market with a 36 percent share, the same figure it achieved the year before. NetWare dropped slightly, from 26.4 percent in 1997 to 24.1 percent in 1998. Other varieties of Unix had a combined share of 17.4 percent. (Smith, 1999)

So what if commercial trends continue to move toward Linux? The author is concerned that if the industry selects Linux as their operating system, the Navy could end up with a lot of legacy Microsoft software that will need to be replaced. As a result, it is this author's opinion that the Navy should choose an architecture that does not rely on vendors or a vendor-based standard.

G. CHAPTER SUMMARY

It is easy and somewhat intuitive to think that a single vendor standard will rid the Navy of its information technology interoperability and economic ills. However, the author believes that the single vendor standard will not be able to quell these problems. As Gartner Group analysts, Altman and Austin describe in their research note *A New Architecture Must Cost-Justify a Technology Shift (1998)*,

> While a single-technology-standard approach appears to offer the easiest way to maintain control, its downside is the resulting dependence on a single vendor as well as technologies being stretched beyond their 'sweet spots.' Also, such standards are frequently set without allocating funds for their implementation, and as a result, they are often quietly ignored.

Clearly individuals do not have the option to ignore policy in the military. As a result, the Navy could end up with systems that are degraded or limited in functionality because it does not have the money to fully fund and maintain these systems.

The Naval Virtual Internet (NVI) (1997) document claims that its principal objectives are, "...to enhance Naval war fighting capabilities and reduce operating costs to all ashore and afloat commands, both within the continental United States and

throughout the world...," but costs could increase with the purchase of a single vendor-based standard. Furthermore, if the hidden costs of Windows NT and vendor lock-in are considered, the author believes IT-21 could end up costing the Navy much more than anticipated.

While Linux was the example used in this chapter, the author believes other operating systems, platforms, or "best-of-breed" products could be substituted in a *heterogeneous* computing environment to realize similar cost savings while maintaining interoperability. The question is not what operating system is better. The question is whether an operating system, or other application, can be used in a particular situation if it makes sense to use it in that situation. With a homogeneous vendor-based standard however, there is only one vendor authorized for use. Unfortunately, there is no IT "Silver Bullet." As Gartner Group analysts Altman and Austin (1998) state,

> Selecting one technical architecture can work well for a while. However, many things can upset this strategy, including a merger or acquisition, the implementation of a major new packaged application, or a critical failure by the key technology vendor. When such events occur, most organizations regress to the chaos level. Less than 25 percent do not...For large organizations, a pluralistic strategy is a form of 'reality therapy.' Although not 'elegant,' it recognizes that no single technology-specific strategy will suffice for all situations. (Altman and Austin, 1998)

In the author's opinion, the Navy would benefit from the recognition that no single technology-specific strategy will suffice for all situations. This will allow a change in mindset from trying to obtain 100 percent compliance with the standard to one of learning how to manage a heterogeneous computing environment. In the author's opinion, once the Navy is able to learn how to strictly manage its heterogeneous computing environment, it will be able to reach the Fifth Stage of Information Technology Transition detailed in Chapter II. In this stage, "Architecture and governance models are well understood, complexity is well managed, costs stabilize, and user voluntarily align with the IT strategy. (Hess and Redman, 1998)

IV. IT-21 SECURITY

A. INTRODUCTION

One of the underlying themes of the *Information Technology for the 21st Century (IT-21)* policy is removing "stove-pipe" systems while driving everything to a single operating system/single PC standard. This policy was designed to reduce costs and increase United States Navy/Marine Corps-wide information system interoperability. Before the United States Navy can achieve interoperability, however, it must have a secure information system architecture. According to Russell and Gangemi (1991) a secure system, or information system security in general, is comprised of, "...*secrecy* (sometimes called confidentiality), *accuracy* (sometimes called integrity), and *availability*." The Department of the Navy (DON) is aware of these security requirements and confirmed their commitment to the inclusion of these security details in the *Information Technology Standards Guidance (ITSG)* document. The *DON ITSG* (1998) states that, "In general, DON information systems should provide appropriate safeguards to ensure the confidentiality, integrity, availability, authenticity, and non-repudiation of information processed."

While every system requires varying degrees of secrecy, accuracy, and availability, each are present, or should be present, in every information system. The military is very familiar with the need for secrecy and the need for accurate information. Confidentiality and integrity are the basic tenets by which the military operates. It has to be this way or operational plans will be compromised and lives will be lost. However, an arm of the security triad that is often overlooked in information system security policies is—*availability*. Availability is becoming increasingly important as the military becomes more reliant on their information systems, and as a result, Chapter V of this thesis has been devoted to the discussion of this topic.

In trying to identify the security concerns of the IT-21 policy, it is appropriate to examine Windows NT security in greater detail. This chapter will focus on the attributes of a secure system and detail the confidentiality and integrity risks associated with the single operating system/single PC concept. Examples will be given to highlight the specific security concerns associated with the Windows NT standard. In addition, other risks associated with the United States Navy IT-21 policy will be noted and suggestions will be made to help the Navy mitigate these security risks.

B. SECRECY/CONFIDENTIALITY

The United States Navy has for long been concerned with the secrecy or confidentiality of information. Secrecy is required to protect the sanctity of operational plans and to protect the national security interests of the United States. "In highly secure government systems, *secrecy...*," as defined by Russell and Gangemi (1991), "...ensures that users access only information they're allowed, by the nature of their security clearances, to access." (Russell and Gangemi, 1991) To help enforce this secrecy, the military has set up a system of classifications to protect sensitive documents and the Navy uses encryption to protect sensitive communication links. With information systems, the Navy uses a firewall and intrusion detection systems to help keep intruders out of its system and to aid in the protection of its secrecy. As the NVI (1997) document states, "The firewall forms the basis of what is described as the force firewall. Intrusion monitoring devices will be operated at the firewall to detect attempts to intrude on shipboard networks." However, in the author's opinion, many administrators often put too much faith in the fact that they have a firewall. They become complacent with the idea that they have a firewall installed and therefore—their system is secure. While firewalls are a good deterrent to unwanted access to computer systems, they are by no means the panacea of computer security. As Behar (1997) notes in *Fortune Magazines* article, "Who's Reading Your E-Mail?," "Some 30% of all break-ins involving the

Internet took place despite the presence of a firewall." While a firewall provides some protection, its mere presence does not protect the secrecy or integrity of United States Navy information. Furthermore, as the FBI notes, "Almost all attacks go undetected—as many as 95%...What's more, of the attacks that are detected, few—perhaps 15%—are reported to law enforcement agencies."(Behar, 1997) In the author's opinion, the Navy must not bank on the fact that its firewalls and intrusion detection systems will keep its information secure. Given that 30% of break-ins occur despite the presence of a firewall and 95% of attacks go undetected, the Navy should continue to be vigilant, even with the "defense-in-depth" concept. The author questions whether the "defense-in-depth" concept will, or should, create a situation where a break-in creates a "so what" condition as claimed in the NVI document.

1. NSA C2 Security Classification

One of the reasons for the inclusion of Windows NT and exclusion of other operating systems in the IT-21 and ITSG policies is the C2 security classification given to the operating system by the National Security Agency (NSA). Is the Windows NT C2 certification all that it is purported to be? The answer to this question depends on whom you ask. If you believe the vendor, of course it is. It is probably wise, however, to be skeptical and recognize the Gartner Group's conclusion that, "...Microsoft is not in the security business and responds to security issues only to the degree and manner that fits the company's business model." (Smith, 1998) It is this type of skepticism that the author believes will help the military reach the security required to protect the secrecy, integrity, and availability of its information systems. The military should try to sift through the marketing hype and concentrate on the true facts of the security offered.

When Microsoft was searching for the National Computer Security Center (NCSC)/National Security Agency (NSA) C2 certification for Windows NT 3.5 with Service Pack 3, they employed a man by the name of Ed Curry to help develop a set of

hardware security diagnostics for Windows NT. In the mid-1990's, Mr. Curry wrote a C2 Rating Maintenance Phase (RAMP) program for Microsoft to aid in the C2 certification process. In 1995 a Microsoft spokesperson said that Curry's contract was ended for reasons that, "...we can't divulge due to our lawyers recommendations." (Foley "New Security", 1998) Curry was concerned about the efficacy of Microsoft's C2 certification process and in a letter sent to the Secretary of Defense, William Cohen, Mr. Curry said, "...his C2 certification contract was discontinued by Microsoft because he refused to lie about Microsoft's violations of C2 guidelines." He went further to add that, "Microsoft has knowingly and willfully concealed information regarding security flaws in computer hardware from the NSA out of fear that revealing such flaws would reduce the number of copies of its products that would be purchased by the government." Curry also stated that he brought up these issues with Microsoft, "...and in return have been the subject of both bribes and threats." (Foley "New Security", 1998) Microsoft responded to Mr. Curry's assertions by stating that, "Ed's [Curry] making a mountain out of a molehill." (Foley "New Security", 1998)

If one examines recent testing by the government, it could be argued that Mr. Curry might not have been too far off in his assessment of Microsoft's certification programs. Microsoft recently failed a cryptography test while trying to get FIPS 140-1 qualified. Microsoft officials acknowledged that, "the lab scrutiny exposed shortcomings in Windows NT's cryptographic processing that will force Microsoft to redesign the operating system." (Messmer, 1999) This redesign could potentially produce interoperability problems and prevent the use of some programs (e.g. Internet Explorer 4.0, Outlook 98, and perhaps other applications). Furthermore, the manager of security technology at the National Institute of Standards and Technology (NIST) warns that, "Government agencies–in theory–shouldn't be using NT to protect sensitive but unclassified information because it isn't FIPS 140-1 certified." (Messmer, 1999)

Microsoft had to be prodded by the Department of Defense to meet the government encryption standards, and as a spokesman for Microsoft confessed, "We got into this a bit late...we weren't effectively paying attention." The author believes this admission gives credence to Gartner Group's assertion that Microsoft is not in the security business, and that it shows a lack of original concern on Microsoft's part for taking security serious. However, in the companies defense, Microsoft said "NT 4.0 and NT 5.0 will henceforth be designed around FIPS 140-1," (Messmer, 1999).

This problem is probably not exclusive to Microsoft. This is most likely true for other commercial-off-the-shelf (COTS) software vendors as well. The author has no way of knowing how much of Mr. Curry's assertions are true, but with the inconsistencies in C2 certification and FIPS 140-1 testing, and given that the Navy's infrastructure is standardized on this single operating system, it is the author's opinion that these claims should be investigated to determine their validity and applicability to the Navy information system architecture. Failing to do so might put the Navy's computer systems in security jeopardy.

Mr. Curry raised questions as to the efficacy of Windows NT C2 certification, and as a result, the author believes the following details are important to help the reader glean a better understanding of the process surrounding the certification. To begin, the Final Evaluation Report conducted by the National Computer Security Center stated the following. The certification was conducted for Microsoft, Inc., for Windows NT Workstation and Server version 3.5 with U.S. Service Pack 3. The platforms that were evaluated were the Compaq Proliant 2000 and 4000 and the DECpx AXP/150. To meet the C2 level requirements it was necessary for the system administrator to, "...disable the OS/2 and POSIX subsystems. Also, the evaluated configuration excludes Windows NT's networking capabilities."

The Navy could hardly use Windows NT in a client/server environment without its networking capabilities, yet that is what is required for it to be C2 certified. In addition, all new versions of an operating system must obtain C2 certification, and to this date, Windows NT 4.0 has not. So in all practicality, Windows NT is not C2 certified for how the United States Navy is using the operating system. The Navy is using version 4.0 of the operating system (not certified) and they are using it in a networking capacity, which would not be certified. It is the author's opinion that, to claim that Windows NT is C2 certified does the Department of the Navy (DON) a disservice because there are probably a number of inexperienced network managers in DON that will be given a false sense of security by such action.

2. Windows NT Maturity

A lot of operating systems have security problems, and the more an operating system is used, the more security holes will be discovered. A lot of Windows NT's problems stem from the fact that it is a relatively immature operating system, as it relates to the length of time it has been in existence, and it is being continually updated to provided increased functionality. Unix, on the other hand, has been around since 1969 when Kenneth Thompson and Dennis Ritchie, system engineers at AT&T's Bell Labs, created the Operating System. Unix was made commercially available in 1977 after several years of increasing popularity. At the same time that AT&T was producing their version, the University of California at Berkeley team was working to improve Unix. They released the Berkeley Software Distribution (BSD) in 1977. The Windows NT project was launched in October of 1988. The first version of Windows NT (version 3.1) was released in August 1993 to coincide with the current version of Microsoft Window's at the time. Normally, new versions of software are given the version number 1.0, although this numbering scheme has changed of late as software vendors have been giving the name of the year that the product is released, instead of the version number

(e.g. Windows 95, Quicken 99, etc.). As a result, Microsoft Windows NT is only six years old. Compare that to Unix, which is 30 years old. While time alone does not make up the whole of an operating systems maturity, it does provide more time with which to test the security of that operating system. Since the current version of Windows NT is version 4.0, the operating system has only undergone one, or at most two, major revisions. As such, Windows NT is a relatively immature operating system in that it has not been around long enough to have been thoroughly tested for security bugs.

3. Microsoft's "Good Enough" Development Strategy

Not only is Windows NT an immature operating system in regards to the length of time it has been in existence, but it is complex. "NT 5.0 will soon break the 20 million-lines-of-source-code mark...Any OS of NT's success and youth will have security holes, and Microsoft's good-enough development methodology only exacerbates those weaknesses." (Smith, 1998) When the Navy established Windows NT as their single operating system standard, they also received Microsoft's "good enough" development strategy and all the problems associated with that strategy. Microsoft's "good enough" strategy, "...revolves around identifying mass markets quickly, introducing products that are 'good enough' (rather than waiting until something is 'perfect'), improving these products by incrementally evolving their features, and then selling multiple product versions and upgrades to customers around the world." (Cusumano and Selby, 1997) What does this mean for the consumer—more money! The more versions and upgrades that Microsoft produces, because they are either fixing previous bugs or adding new features, the more money it will cost the military. By their own admission, Microsoft is driven by increasing functionality and product innovation. This programming climate often runs counter to the security and stability of the operating system.

"The risks of 'good enough' computing lie primarily in two areas. Firstly, there are risks in the *potential* mismatch between the real requirements of the enterprise for

performance and high availability and the ability of the platform selected, and the implementation choices made to satisfy those requirements." (McGuckin, 1998) As the reader will discover in Chapter V of this thesis, there is likely a mismatch between the requirements of the United States Navy and the vendor specific single operating system/single PC standard. "Reference checks of vendor proposals should always test whether the enterprise is entering uncharted territory: exceeding the current high water marks for users supported, database size or uptime characteristics by more than 10 percent radically increases the risk of using a specific server platform." (McGuckin, 1998) As described in Chapter V of this thesis, at this time Windows NT is not as reliable as the Navy requires. (However, Microsoft is a robust company and is probably working on these problems for the next revision of their operating system). In fact, the uptime characteristics of Windows NT are not close to the 10 percent required to keep from radically increasing the risks of using a specific server platform. Windows NT's availability is 10 times worse than Unix and other commonly used platforms, making its adoption as the single operating system standard, in the author's opinion, an extreme risk.

The second risk associated with "good enough" computing lies in the hidden costs that might be incurred.

> For example, users who have a 24X7 service-level requirements and who decide to implement manual fail-over have often not budgeted for three shifts of senior-level systems administrators. They may opt to rely on on-call administrators when failures occur on the nonprime shift (which could result in inordinately long downtime). Alternatively, they may incur additional systems management costs by increasing the number of administrators watching over their systems. (McGuckin, 1998)

The hidden costs of Windows NT might be adding more costs than the Navy is aware. In a survey of early Windows NT adopters, those who are arguably the most loyal to the platform, some 75 percent exceeded their multi-server Windows NT deployment budgets by more than 40 percent. Of those 75 percent, 25 percent actually went over

budget by greater than 80 percent. (Weiss, 1997) These hidden costs could add significant expense to the total cost of ownership of the Navy's single vendor-based standard—Windows NT.

Another problem with Microsoft's development strategy is that Microsoft has been working under the single user, single machine mentality. This mentality is often hard to change, but it is a required change when making software for enterprise level organizations.

> Although the situation is changing, it's evident that Microsoft's NT developers are still working from the premise that a single user will use a single dedicated computer. This mindset assumes that if a machine crashes or is compromised, that failure will affect only one user and one computer. The one-user, one-machine scenario use to fit word processors and spreadsheets, but the nature of enterprise computing has changed drastically. At least in situations in which security is concerned, we're not in Kansas. (Smith, 1998)

Since the Navy will be working in a network-centric world, it is the author's opinion that the Navy will not be able to stagnate in Microsoft's one-user, one-machine world. Multi-user applications will be a requirement and the security concerns of multiple users will have to be taken into consideration. When a failure occurs in an enterprise level architecture it does affect others in the architecture, especially if that failure is at the server level.

4. NT's Top Security Problems

In his article, "NT's Top Security Problems," Smith (1998) of *Windows NT Magazine*, details Windows NT's top security problems as stated by the Gartner Group. Table 4.1 below identifies the specific security problems associated with the Windows NT product. These problems, and their relationship to the United States Navy, will be explained in detail in the paragraphs that follow.

Table 4.1: NT's Top Security Problems

Problem 1:	Domain Complexity
Problem 2:	Administrator Account Does Not Lock Out
Problem 3:	No Default Auditor Account; Administrators Can Alter Audit Logs
Problem 4:	NT Allows Remote Administration
Problem 5:	Poor Audit-Logging Capabilities
Problem 6:	Default Guest Account
Problem 7:	No Salt in the Password Mix

From Smith, 1998.

a. Domain Complexity

Having studied to complete the Microsoft Certified Systems Engineer (MCSE) exam series, the author can attest to the difficulty involved in learning how the domain and trust relationships operate in the Windows NT environment. Microsoft most likely understands this complexity as well, as they are changing to a directory system (Active Directory) similar to that produced by Novell. Seeing as this will be Microsoft's first implementation of a directory system, the author can envision a bumpy road ahead. As Smith (1998) said,

> Many administrators (and even some Microsoft engineers) lack a complete understanding of how various NT components (e.g., workstations, member servers, and domain controllers) cooperate in a single- or multi-domain environment. This incomplete understanding often leads to a more complicated and costly computing environment than necessary. (Smith, 1998)

Much of the justification of moving to the Windows NT standard has been based on the fact that Windows NT has a Graphical User Interface (GUI) and it is supposed to be easier to operate with a lower Total Cost of Ownership (TCO). These TCO arguments have been adequately addressed in Chapter III of this thesis and have been shown to be not necessarily the case. As far as the graphical user interface, just because one has a GUI, doesn't mean that the operating system is easy to operate.

Knowing DOS is still very helpful with Windows NT deployments and is, or should be in the author's opinion, a required piece of knowledge for system administrators. Furthermore, system administrators will need to have the knowledge contained in the MCSE certification series at a minimum. The system is too complex and there are too many variables. With the United States Navy moving to an all Windows NT standard, system administrators will have many domains that will need to be managed and trust relationships that will need to be set up with and between these domains. This increased complexity will make for a less secure environment. As Smith (1998) states, "With fewer domains, you enhance security and reduce costs because you have fewer trust relationships to manage and fewer domain controller systems to purchase and maintain, and you have less potential for inconsistent administration practices and policy between domains." (Smith, 1998)

b. Administrator Account Does Not Lock Out

One of the problems with COTS software is that it is made for the consumer. Does that sentence sound a little weird? Something is a problem if it is made with the consumer in mind? Well the answer is yes, because ease of use is paramount when developing software for the consumer. Why is this a problem? Ease of use is often at the opposite end of the spectrum from security. It is sometimes viewed that on a spectrum of security and ease of use, security lies on one end and ease of use on the other—and in the middle the two shall rarely meet. As such, in the author's opinion, the United States Navy should be careful when employing COTS software. Windows NT is no exception. As Smith 1998 points out, "It's true that, out of the box NT never locks out the administrator account, even if account policies enable this feature. However, you can use PASSPROP, a command-line program in the *Microsoft NT Server 4.0 Resource Kit* [requiring knowledge of DOS], to enable account lockout for remote logons that use the administrator account." Why is it important to be able to lock out the administrator

account? Well, if a hacker is trying to hack into your system remotely, they can hack at will until they get in. There is no limit on the number of times they can try passwords. Normally, a limit would be set, (e.g. 3 logon attempts), before the account would be locked out. This is not a default setting out of the box. In order to have secure information systems, system administrators must keep up-to-date and keep their systems up-to-date.

This brings to light another concern the author has with the IT-21 policy, there is no mention of management related issues. Since most of the cost of information systems is in the administration of that system and end-user functions, as detailed in Chapter III, it seems logical to the author that the Navy could reap greater return on its investment with a more defined management strategy.

If the Navy is to fight future wars using Network Centric Warfare, information systems will be paramount in facilitating that endeavor. "More than a year ago, a program appeared that demonstrated how to discover a built-in administrator account name with nothing more than access to the target system via NetBIOS over TCP/IP. The program is called Red-Button, and it exploits a capability in NT that lets anonymous logon users list domain usernames and enumerate share names." (RedButton as well as other hacker attacks led to the nickname of "Security Pack 3" for Windows NT Service Pack 3). Letting the enemy see the makeup of the Navy information system architecture is not a very secure way to go about doing business as far as the author is concerned. If the Navy is not keeping up with the latest fixes then its systems are not going to be secure.

c. *No Default Auditor Account; Administrators can Alter Audit Logs*

Not only does the Navy need to be concerned with security from outside agencies, but it also needs to be conscious about security from insider attacks. Insider

attacks are a common form of security breach and some of the hardest to see coming. While the author believes in the integrity of everyone in the military, there have been times when insiders have inflicted grave damage to the national security interests of the United States (e.g., Aldrich Ames, Jonathon Pollard, and Robert Walker). Had these men had the resources, the knowledge, and the "insider advantage," they could have inflicted grave damage to the security of our information system architecture.

> NT's implementation of C2 security doesn't distinguish between an administrator and an auditor. In an ideal system, all administrator and user actions would be logged for later review by an auditor, and no users, including administrators, could cover their tracks by altering the logs. Currently, NT can log administrator actions, but there are several ways administrators can hid those actions. (Smith, 1998)

This includes administrators that have gained administrator privileges illegally, effectively allowing a cracker with administrative privileges to erase all of his tracks.

d. Windows NT Allows Remote Administration

One advantage for system administration is the ability to manage systems remotely. Remote administration provides ease of responding to trouble calls and should help reduce support costs. The problem with remote administration is that one introduces added security risk into an information system. Gartner Group recommends a policy of not allowing remote Windows NT administration because you, "...increase the risk to your system security when you let administrators connect to servers over the network." (Smith, 1998) Not allowing remote administration posses a problem with the Total Cost of Ownership (TCO) argument. If system administrators are not able to conduct business remotely, they do not reap the benefits of centralized administration, which could end up increasing the TCO of the information system.

e. Poor Audit-Logging Capabilities

Windows NT also has poor audit-logging capabilities out of the box. The author believes these capabilities are not acceptable for enterprise use, and as such, are not acceptable for the United States Navy.

> Gartner Group recommends using third-party tools to overcome what the group perceives as a security weakness in NT...NT has no native way to get comprehensive view of network activity. Take, for instance, logon activity events. If you want to see all failed logons in your domain, you must look at the Security Log of every server and workstation. (Smith, 1998)

Is the Navy going to send a system administrator to each workstation to check for this suspicious activity? Clearly this is not an acceptable option. In the author's opinion, the Navy should purchase third party tools to do the job instead. However, if multiple items have to be purchased as add-ons to the operating system to increase its security, these items should be included in the TCO of Windows NT to give a more realistic view of what the operating system actually costs.

f. Default Guest Account

Another security concern associated with Windows NT is that;

> NT comes with a built-in guest account, and Gartner Group questions whether this default guest account is necessary. This account lets users who do not have regular accounts log on. The bad news is that the guest account allows anonymous access. However, the guest account is disabled by default in NT Server, mitigating the account's inherent risks. (Smith, 1998)

While this problem seems fairly innocuous, an unsuspecting system administrator could enable this feature and open up a Pandora's box of insecurity. With the guest account active, those outside of the Naval Intranet could gain access by logging in as guest with no password.

g. No Salt in the Password Mix

Mr. Smith (1998), the author of "NT's Top Security Problems," an article in the October 1998 issue of *Windows NT Magazine*, "...has been implementing distributed solutions to meet mission-critical enterprise security requirements for a decade. He provides NT security training and consulting." Even though Mr. Smith has ten years of security experience, and has detailed several relevant security issues with Windows NT, he doesn't know it all. No one does. Herein lies the problem with securing United States Navy information systems. The more complex the Navy makes its information systems, the more difficult it will be to secure those systems, and the more information individual system administrators will have to know in order to provide that security. The reason why the author states that Mr. Smith doesn't know it all is that he said, "I suspect Gartner Group means by no salt that NT doesn't enforce quality password policies. By default, NT has no password requirements. However NT has a rich set of password features that administrators can use to set strong password policies, which Gartner Group recommends." Mr. Smith then goes on to explain how Windows NT provides password quality, through change frequency and other policies. What Mr. Smith does not understand, despite his years of experience, is the meaning of "salt" in the password mix. "Salt" in the password mix is the process of putting variability into the encrypted passwords so the encrypted passwords are not the same. If two users have the same password, and that password is then encrypted for storage in a password file, and if those two passwords are the same, then the encryption of those passwords would also be the same without "salt." If a person gains access to the Windows NT password file and discovers that two of the encrypted passwords are the same, then those passwords are probably easy to guess/break. Table 4.2 below illustrates the concept of "salt" in a password.

Table 4.2: "Salt" in the Password Mix

Password	Salt	Encrypted Password
gonavy	No Salt	afKC4Niknte2B
gonavy	No Salt	afKC4Niknte2B
gonavy	With Salt	8nvoDB24fdscF
gonavy	With Salt	4nf43daWlE32c

The fact that two of the encrypted passwords are the same means that at least two people have guessed the same password. It is likely that the password is constructed of easy to remember dictionary words and could be cracked in a matter of seconds on a computer with a program like LOphtCrack. In the author's opinion, every system administrator in the United States Navy should have these hacker tools and run them on their own system to see where vulnerabilities lie and learn how to better secure their information systems.

C. ACCURACY/INTEGRITY

"Windows NT administrators should be on the lookout for a new strain of computer virus that can wreak havoc on their networks. Referred to as the Remote Explorer virus, this malicious mobile code encrypts executable, text and HTML files on NT systems, rendering the files unreadable." (Burns, 1999) This particular virus only targets Windows NT Server and Windows NT Workstation, but may be carried, like a parasitic host, by other operating systems. The first known case of the virus was detected in December 1998 by MCI WorldCom and it reportedly spread to, "...10 of the company's sites and affected several thousand NT servers and workstations." (Burns, 1999) But how could this happen? The author is quite sure MCI WorldCom uses anti-virus software. This virus works by tapping into Windows NT's remote administration feature and since it's a new virus, it was able to slip through anti-virus software. If a

virus can affect thousands of computers in a respected corporation like MCI, it can surely do the same to military systems—especially if they all have the same operating system. The results of this virus can be devastating as the integrity of mission critical data can be breached. This could ultimately result in lost man-hours and lost data as information could be irrevocably changed.

"*Accuracy* or *integrity*...," as defined by Russell and Gangemi (1991), "...means that the system must not corrupt the information or allow any unauthorized malicious or accidental changes to it. It wasn't deliberate, but when a simple software error changed entries in Bank of New York transactions several years ago, the bank had to borrow $24 billion to cover its accounts until things got straightened out—as the mistake cost $5 million in extra interest." Normally, access must be gained into the system before the integrity of the data can be changed. As a result, the threat to the accuracy of Navy information, or the integrity of Navy systems, will most likely come from within. These threats do not have to come from malicious intent. Computer users, and system administrators alike, can engage in activities that could accidentally cause a decrease in the accuracy or integrity of information. System administrators could damage files during upgrades to system software and users could accidentally delete files for which they have access to delete. Fortunately, with mandatory back-up procedures, the results of these breaches in integrity can be recovered to full operational status. However, time and manpower must be expended to recover the damaged files, creating an additional hidden cost for system integrity violations.

1. Identification and Authentication

As access must be gained before the integrity of the data can be changed, it becomes very important that users are properly identified and authenticated. In almost every system that has a user identification and authentication method to access a computer, the security of the system ultimately rests with the individual user. If the

individual writes their password on a sticky-note and sticks it to their monitor, free access is available to get into their account. Crackers can also steal passwords and break them in order to gain unauthorized access to information systems, thus threatening the information systems integrity.

> In an incident recently reported to the CERT/CC, a very large collection of password files was found on a compromised system. In total, the intruder appears to have a list of 186,126 accounts and encrypted passwords. At the time the password file collection was discovered, the intruder had successfully guessed 47,642 of these passwords by using a password-cracking tool. (CERT/CC, 1998)

The login names and passwords give the cracker the keys to the unsuspecting victims account—and all the permissions that the account affords. To prevent infractions of integrity, the Navy, in the author's opinion, should establish a good password policy that stresses end-user involvement in the security of those passwords.

> The bottom line is that neophyte hackers can download tools such as LOpht-Crack for free from the Internet and gain access to your accounts if they can get a copy of your password hashes. NT stores password hashes in as many as seven locations, and tools such as LOphtCrack can currently find and crack hashes in all but one of the locations. You need to be aware of the risks involved with storing passwords in each location and measures you can take to protect your network from hacker attacks. (Smith, 1998)

2. Threat from Foreign Powers

Is the United States Navy really worried about the 14-year old hacker that breaks into their system? Probably, but that type of hacker is a mere annoyance compared to a dedicated threat from a foreign power. Adversarial countries can educate a small number of hackers to penetrate United States information systems without a huge outlay of cash. They can create High-Energy Radio Frequency (HERF) weapons/devices, from household components, and those purchased from Radio Shack, to disable computer

equipment. They can also get information off of the Internet to make a van Eck device. A van Eck device could allow our adversaries to eavesdrop on our video display units from several hundred meters distance, using only a normal black-and-white TV receiver, a directional antenna, and an antenna amplifier. Distances of over one kilometer can be achieved with more sophisticated receiving and decoding equipment. As a result, countries with little to no economic resources can now become threats to the United States national security interests. They just have to assemble a small team of well-educated hackers. This type of threat from foreign sources is not far from reality. In fact,

> On July 4, 1997,the Russian developer Konstantin Sobolev released a utility [*getadmin*] on the Internet that allowed any user on a Windows NT computer to be added to the administrators group...Within days of Microsoft's release of a hot-fix, another researcher, Constin Raiu, had posted additional exploit code which permitted *getadmin* to still function. In this instance, Raiu's Internet electronic address and Web site were in a foreign domain. (McDonald, 1998)

The threat from foreign powers is real, and in the author's opinion, the Navy should be vigilant in its efforts to counter such threats. DOD should be careful not to put too many of its security eggs in one basket. Even with one of the more secure database systems, Oracle, "Sixty-two percent of the time that auditor Gordon Smith breaks in to a corporate network with an Oracle Corp. database, his team easily gains full control of that database. The reason: Nobody bothered to change the default administrative password that ships with Oracle software." (Machlis, 1997) In the author's opinion, the United States Navy should ensure that instructions and standards are in place to walk all network administrators through the secure setup of all applications, system software, and hardware, if they expect their security features to work. Security features are of not much benefit to the United States Navy if they are never turned on. There are products that the United States Navy has developed that will step system administrators through the

process of making Windows NT secure, but how many system administrators know they exist, know how to get them, and know how to implement them?

D. CHAPTER SUMMARY

In the author's opinion, the Navy needs to balance cost, ease of use, and a host of other issues, with the security concerns associated with its information systems. System administrators need to be trained and made aware of all aspects of the security of their information systems. However, that is not happening in some situations. According to a 1997 Government Accounting Office survey, "Many military installations lack full-time data security officers...and a number of systems administrators surveyed said they hadn't received any formal network security training."(Machlis, 1997) Furthermore, according to a report released by the National Research Council (NRC), a nonprofit agency that offers science advice under a Congressional charter, the Department of Defense is "...lagging behind in securing its systems from cyberattacks." While the agency commends the military for its physical security, it found that the military does not have adequately trained personnel in information system security related matters. In fact, during a recent exercise, "... personnel in an operations center mistook a cyberattack for a joke." (Ohlson, 1999) How can the Navy expect its system administrators to fight cyber wars and live in a network-centric world when they are not being trained how to defend their information systems from attack?

In the author's opinion, the Navy should remain alert and ensure its system administrators are adequately trained for the job that they are being asked to do. The Navy should do this because, as Cliff Stoll says in his book *The Cuckoo's Egg* (1990), the hacker is like a cuckoo who, "...lays her eggs in other birds' nests. She is a nesting parasite: some other bird will raise her young cuckoos. The survival of cuckoo chicks depends on the ignorance of other species." Let's not let ignorance about information system security put the Navy at a disadvantage to its adversaries. Let's not let ignorance

nurture that young cuckoo. The Navy should choose security policies and provide security training that will provide for a more secure information technology architecture because "The only secure computer is one that is turned off, locked in a safe, and buried 20 feet down in a secret location—and I'm not completely confident of that one either." (Behar, 1997)

V. IT-21 AVAILABILITY

A. INTRODUCTION

While the *Naval Virtual Internet (NVI)* document (1997) states that, "The fundamental requirement of NVI computing services is to provide universal, reliable user access to information, and enable the user to produce information, when necessary...," the document does not really address availability or reliability beyond the mere mention that it is required. Availability is an often-overlooked aspect of computer security, but it is becoming more important as the costs of downtime have greatly increased for enterprises reliant on their information systems. These costs are blindingly apparent to the online auction web site eBay. According to Bloomberg Television in June of 1999, eBay experienced a 22-hour outage of its service, which caused a 30-point drop in its stock price and cost the company between $3 and $5 million dollars in revenue.

While it is easier to translate this downtime into dollar figures in the private sector, the military also has a lot at stake in the availability of its information systems—the lives of sailors and soldiers. The importance of availability in the military became apparent during the recent bombing campaign over Kosovo. PC users in Belgrade conducted denial of service attacks against the NATO public-information web site thus making it unavailable to legitimate users. (Diederich, 1999) While this was just a public information site, it highlights the dangers that lurk if adversaries are able to deny the military access to its operational information systems.

Another concern the author has with the move to a single PC (Intel) and standardization on a single operating system (Windows NT4.0/2000), is that the Navy is inviting availability problems that could greatly degrade its mission readiness and effectiveness. These standards could potentially keep those soldiers and sailors from producing the timely information that is often required by operational commanders.

Having a single operating system and a single PC standard could negate the redundancy benefits of the "defense-in-depth" concept by allowing a Single Point of Failure (SPOF) or Common Cause Failure (CCF) in the Navy information system architecture. This chapter will focus on the availability concerns of a homogeneous vendor-based computing standard, and more specifically, the availability concerns of choosing Microsoft Windows NT as that standard.

B. AVAILABILITY

The more the Navy uses information systems, they more it becomes reliant on those systems, and the more operational commanders will demand that they work when they are called upon to be used. Some in the Navy have become so reliant on computers that one might claim that email is a "mission critical" system—and it might be in some instances. As the Navy moves from platform-centric warfare to network-centric warfare, sooner or later, it will begin to view information systems as "mission critical." Information systems make up the basic components of a network-centric system, and as such, it is the author's opinion that is should be given the funding and priorities that other weapon systems or platforms are now given. As the Navy continues its migration toward network-centric warfare, operational commanders will become more reliant on information systems to fight the battles, "see" the operational picture, and aid in decision making. As the Navy moves towards network-centric warfare, the Navy should treat it just as that—warfare. In the author's opinion, the Navy should apply the lessons learned in previous wars and ensure that it has diverse and redundant systems that eliminate single points of failure or common cause failures in its information systems. If the Navy will be fighting future wars in cyberspace, it will need to make sure that its information systems are available for use—denial of service will not be tolerated. The availability of United States Navy information systems will become as important, if not more important, than the secrecy and integrity of the information that is contained on those systems.

The importance of availability in military information systems was confirmed during Operation Desert Shield/Storm. As Table 5.1 below shows, during the Gulf War, "Flash" message traffic had an average backlog of 8.6 hours and it took 18 hours before 90 percent of the traffic had been received. Compare these numbers to a pre-Desert Shield/Storm average backlog of 0.6 hours and a one-hour latency before 90 percent of the traffic had been received.

Table 5.1: Desert Storm Bandwidth/Availability Constraints

	Pre-Desert Shield/Storm		During Desert Shield/Storm	
	Average Backlog	90% Recd	Average Backlog	90% Recd
Flash	0.6	1.0	8.6	18.0
Op Immediate	2.9	7.0	8.7	18.0
Priority	6.7	19.0	42.0	135.0

From Brady, 1998.

There was basically no difference between the "Flash" and "Op Immediate" message precedence during the Gulf War. "Priority" traffic was ineffectual. By the time message traffic was received by anyone, the situation would have become, as they say, OBE—overcome by events. Clearly these were unacceptable numbers and signaled inadequate bandwidth and a weakness in the availability of our communications systems—but what is availability?

In Russell and Gangemi's (1991) book, *Computer Security Basics*, "*Availability* means that the computer system's hardware and software keeps working efficiently and that the system is able to recover quickly and completely if a disaster occurs." While these are important aspects of availability, in the military, one also has to take into consideration whether or not a system is operable when it is required to perform a

mission. As such, the Defense Systems Management College (DSMC), *Systems Engineering Management Guide* (1983), definition of availability complements the Russell and Gangemi definition and makes the combination of definitions applicable to the military. The DSMC defines availability as, "A measure of the degree to which an item is in an operable and committable state at the start of a mission when the mission is called for at a random time."

C. NUMBER OF NINES IN AVAILABILITY

On its very basic level, availability is required and needed by everyone wishing to use an information system. Without availability, one would not be able to use their information system and would have no need for secrecy and accuracy. Many do not realize that availability is a part of information systems security. In fact, if one were to ask someone what availability they require in a system, they would probably tell you that 90 percent sounds like a good, or robust, availability figure. Before the author started this research, he thought that 90 percent sounded like a good figure. However, 90 percent availability would actually account for 876 hours or 36.5 days of downtime on average in Navy information systems per year.

When private enterprise talks about availability, they talk about the *number of nines*. The number of nines in the percentage is often used to describe the availability of a system (e.g. four nines would be 99.99 percent). Hewlett Packard's "5 nines—5 minutes'' goal calls for 99.999 percent application availability or just five minutes of downtime per year. The more *nines*, the more money an organization will save, because that organization will not be loosing money waiting for their computer to be repaired, rebooted, or replaced. If these information systems are running fire control systems or shipboard propulsion systems, the author questions if the skippers of those ships would be comfortable with an average of 90 percent availability.

What availability percentage is required for United States Navy information systems? The Naval Virtual Internet Integrated Process Team (1997) stated that, "The core IP and bandwidth services to be provided in the NVI must be 'industrial strength.' It must have high reliability and availability...We need to target a reliability figure of 99.99%." While the NVI IPT was talking about IP and bandwidth services, it is the author's opinion that other equipment will also have to strive to obtain the 99.99 percent (four *nines*) availability figure in order to provide the services required in a network-centric arena. Can these reliability and availability figures be obtained with a single commercial-of-the-shelf (COTS) software/hardware standard?

D. COMMON CAUSE FAILURES/SINGLE POINT OF FAILURE (CCF/SPOF)

To determine the answer to this question, one needs to explore the relationship of common cause failures (CCF), or single points of failures (SPOF), to availability in the Navy information systems architecture. In their book, *System Reliability Theory*, Hoyland and Rausand (1994) define common cause failures, or single point of failure, as, "...multiple failures that are a direct result of a common or shared root cause. The root cause may be extreme environmental conditions (fire, flood, earthquake, lightning strike, etc.), failure of a piece of hardware external to the system, or human error. The root cause is not a failure of another component in the system." In the case of the IT-21 single operating system/single PC standard, a common cause failure, or a single point of failure in the system, could be attributed to either the operating system or the PC platform. Some might think that with today's solid state components, it is not possible for a single PC or a single operating system standard to be a single point of failure in an information system. The examples below will demonstrate how a single operating system/single PC standard could be a single point of failure in the United States Navy information technology architecture.

1. Examples of SPOF in Computing Architectures

In November 1988, Robert T. Morris created the Internet worm, which was a program that took advantage of bugs in the Sun Unix *sendmail* program, VAX programs, and other security loopholes to distribute itself to over 6000 computers on what was then the Internet. The worm itself had a bug which made it create many copies of itself on machines it infected, which quickly used up all available processor time on those systems—effectively bringing things to a screeching halt on the Internet. Had the military standardized on Sun Unix only, it is the author's opinion that this worm would have brought the military to its knees. Many of these networks connected to the Internet at that time found that having a variety of different computers running on their network was an advantage. This is because it is highly unlikely that an infection on one machine would be able to run on a large number of different machines. Therefore, those networks with the greatest diversity had a lesser chance of being completely incapacitated by such an attack.

In another example, dealing with the hardware itself, Intel sold some processors in 1994 containing a math bug. "Not only had Intel officials known about this, but apparently they had decided not to tell their customers until after there was significant public reaction." (Garfinkel and Spafford, 1996). Fortunately for the company, the processor was not in popular use at the time. But let's assume that the United States Navy decided to purchase a standard PC containing that "buggy" Intel chip. Not only would firing solutions be calculated incorrectly, as well as a host of other problems, but the United States Navy would have to make a wholesale replacement of those processors in order to bring the fleet up to working condition—that is, providing the supplier even released the information. In the author's opinion, standardizing on a PC containing a defective processor would pose grave danger to those men and women relying on that

inaccurate information. It would have caused a single point of failure in the Navy's information system architecture.

In a further example, a denial of service attack was perpetrated against Windows NT and Windows 95 machines on the MIT campus resulting in frozen machines, spontaneous reboots, and the infamous "Blue Screen of Death." In response to the attack, MIT noted, "Because of MIT's heterogeneous computing environment, this operating system specific attack only affected a portion of the MIT user community." (1999) There are many other examples of large-scale denial of service attacks, viruses, software bugs, and other attacks that would be the genesis of common cause failures in various information technology architectures. These real world examples, as well as those detailed in the Chapter IV of this thesis, indicate the importance of how a single operating system/single PC standard can cause a single point of failure in the Navy information system architecture.

E. AVAILABILITY USING DIVERSE AND REDUNDANT SYSTEMS

The availability of individual components in a networked system is very important because the availability of the entire system gravitates towards the systems weakest link. If several subsystems are connected together in series, (e.g. router, firewall, server), the lowest availability subsystem will lower the total availability of the complete system. Since no system or component has 100 percent availability, it becomes important to have high availability components in the information system architecture so the overall system availability remains high. In the paragraphs that follow, the author will demonstrate why availability is important to the United States Navy information systems architecture, and how diverse and redundant systems can increase the average availability of Navy information systems.

1. Availability Definition and Equations

In their book *System Reliability Theory*, Hoyland and Rausand (1994) define Average Availability as, "the mean proportion of time the item is functioning. If we have an item that is repaired to an 'as good as new' condition every time it fails, the average availability is" given by Equation 5.1:

$$A_{av} = \frac{MTTF}{MTTF + MTTR} \qquad \textbf{Equation 5.1}$$

Where, A_{av} = Availability (Average),

MTTF = Mean Time To Failure – the mean functioning time of the item.

MTTR = Mean Time To Repair – the mean downtime or repair time after a failure.

Equation 5.1 above can be translated into more useful terms for Navy use in calculating the average availability achieved in its information systems. The equation roughly translates to *UpTime* divided by *TotalTime*. Uptime can be further broken down as *TotalTime* minus *DownTime* as given by Equation 5.2:

$$A_{av} = \frac{UpTime}{TotalTime} = \frac{(TotalTime - DownTime)}{TotalTime} \qquad \textbf{Equation 5.2}$$

This availability measurement can then be applied to components, subsystems, or an entire information system to allow one to compare the relative availability between different information system architectures. If one takes Equation 5.2 above and solves for *DownTime*, the equation becomes:

$$DownTime = TotalTime - (TotalTime * A_{av}) \qquad \textbf{Equation 5.3}$$

In order to determine the total amount of downtime in minutes or hours per year, it is also helpful to have the following two constants stating the total number of minutes and hours in a year.

$$\frac{TotalMinutes}{year} = \frac{365days}{1year} * \frac{24hours}{1day} * \frac{60Minutes}{1hour} = \frac{525600Minutes}{year} \quad \textbf{Equation 5.4}$$

$$\frac{TotalHours}{year} = \frac{365days}{1year} * \frac{24hours}{1day} = \frac{8760hours}{year} \quad \textbf{Equation 5.5}$$

Equation 5.3 will be used in the following example to calculate the downtime of various information systems architectures.

In a simple example, a server is connected to a router which is then connected to a Wide Area Network (WAN) in series, as shown in Figure 5.1 below.

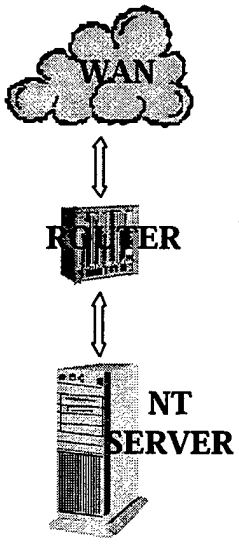

Figure 5.1: Sample Information System

The overall availability of the total information system will be the multiplication of the individual availability of its components. Namely, the availability of the WAN multiplied by the availability of the router multiplied by the availability of the server will yield the average availability of the system, as given by Equation 5.6 below.

$$A_{av(System)} = A_{av(WAN)} * A_{av(Router)} * A_{av(Server)} \qquad \textbf{Equation 5.6}$$

2. Calculating Information System Availability

To demonstrate the importance of eliminating single points of failure (SPOF) or common cause failures (CCF) in information system architectures, the examples that follow will calculate the availability of an information system using one Windows NT server, one UNIX server, two Windows NT servers, two UNIX servers, and a combination Windows NT-UNIX server architecture. The multiple server models will be constructed so that parallel crossover/fail-over points will be connected to enable a more robust system architecture thus showing the advantage of eliminating SPOF.

In order to implement the example information system, the availability of the WAN and the availability of the router are held constant between systems so a comparison can be made between server platforms. An average availability of 99.7 percent will be assigned to the WAN and an average availability of 99.9 percent will be assigned to the router. These values roughly approximate the values that would be found in the normal operation of these components. The availability numbers for the server platforms are taken from real world data contained in the Gartner Measurement database. The Gartner Group data contains availability metrics among the most-used server platforms and is compiled from a group of 240 observations covering 190 firms. This data is enumerated in Table 5.2 below.

Table 5.2: Availability Ranges for Top IT Platforms

Platform	Outages per Server per Year	Availability (24x365 basis)
S/390 (Sysplexed)	10 minutes	99.998%
Tandem	1.7 hours	99.98%
AS/400	5.2 hours	99.94%
S/390 (nonsysplexed)	8.9 hours	99.90%
VAX	18.9 hours	99.78%
Unix (all)	23.6 hours	99.73%
NT	224.5 hours	97.44%

From Fitzpatrick, 1998.

Out of all the availability metrics of the most-used platforms above, one number stands out—the one associated with Windows NT. Windows NT has an availability that is orders of magnitude longer in hours of outages per server per year than any other of the most commonly used platforms. Compare Windows NT's availability to that standard required by the NVI IPT. As shown in Table 5.3 below, the four nines standard set forth in the Naval Virtual Internet document would give .876 hours of downtime per year. Windows NT has 224.5 hours of downtime per year.

Table 5.3: Downtime for the "Nines" in a Percentage

Number of "Nines"	Percentage	Downtime per year (Hours)	Downtime per year (Minutes)
5	99.9990 %	.0876	5.2560
4	99.990 %	.876	52.560
3	99.90 %	8.76	525.60
2	99.0 %	87.6	5256.0
1	90.0 %	876	52560.0

a. Availability of a Single System

When these platforms are put into an information system, these availability numbers can greatly affect the overall availability of the total information

system. Using the information from the previous scenario, the WAN is given an average availability of 99.7 percent, the router an average availability of 99.9 percent, and the server platform is given the average availability information compiled by the Gartner Group above. In this particular case, the Windows NT platform has an average availability of 97.44 percent. This information is summarized in Figure 5.2 below.

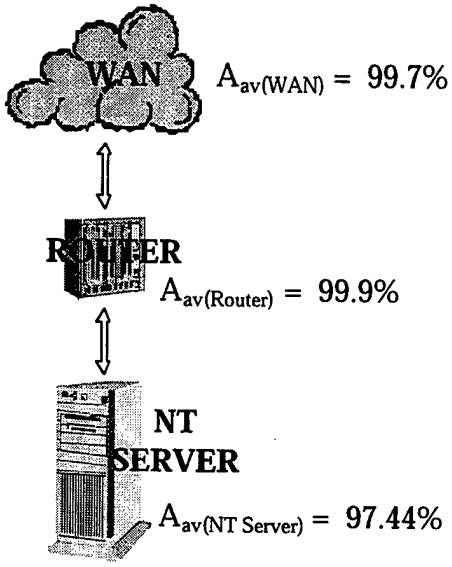

Figure 5.2: Information System with Average Availability Figures

Using equation 5.6, one can calculate the average availability of the information system with an NT server as:

$$A_{av(System)} = .997 * .999 * .9744 = .9705$$

Using this average availability for the entire system, one can calculate downtime using Equation 5.3 and the constants in Equations 5.4 and 5.5. The resultant downtime is given below:

$$DownTime = 525600 - (525600 * .9705)$$

$$DownTime = \frac{15505.2 Minutes}{year} = \frac{258.42 hours}{year}$$

b. Availability of Redundant Systems

To calculate the availability of an information system with crossover/fail-over points for redundancy and diversity, two servers, two routers, and two WAN's are used. Figure 5.3 below represents an information system composed of a Windows NT and UNIX server-router-WAN configuration with crossover/fail-over.

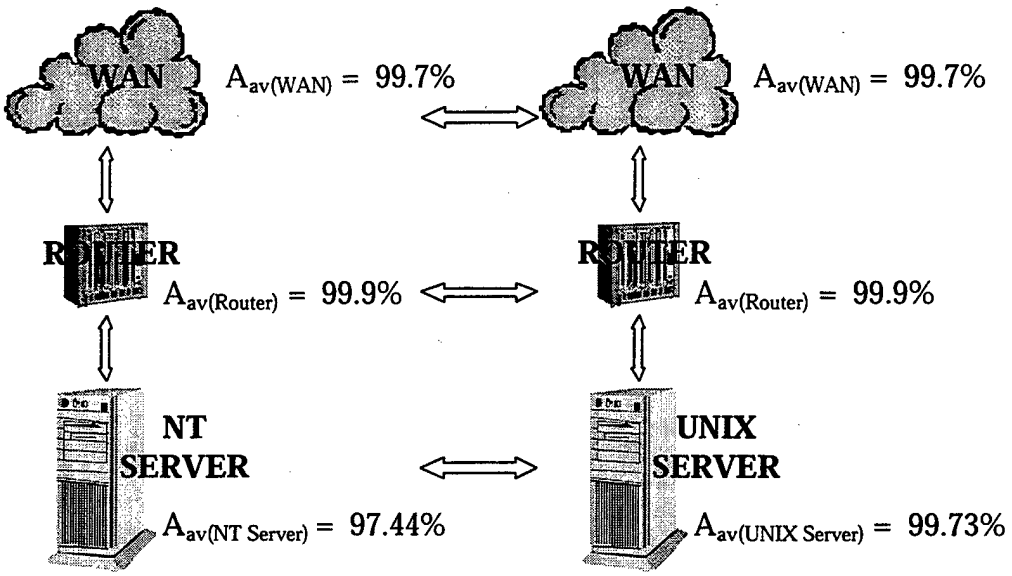

Figure 5.3: Information System with Crossover/Fail-over

In order to highlight the differences between servers, the WAN and router figures in each subsystem will remain constant. By making this assumption, one can determine the contribution to the availability that the servers provide to the total information system. For this information system, comprised of crossover/fail-over links, both servers must fail in order for the entire system to fail. This is represented by Equation 5.7:

$$P(ServerSystemFailure) = (1 - A_{av(Server1)}) * (1 - A_{av(Server2)}) \quad \textbf{Equation 5.7}$$

Using Equation 5.7, the probability of a server system failure is:

$$P(ServerSystemFailure) = (1 - .9744) * (1 - .9973)$$

$$P(ServerSystemFailure) = .0256 * .0027 = .00006912$$

The probability of a server system success, or the availability of the combined servers, is given by Equation 5.8:

$$P(ServerSystemSuccess) = 1 - P(ServerSystemFailure) \quad \textbf{Equation 5.8}$$

Using Equation 5.8, one can calculate the probability of success for each level in the information system as:

$$P(ServerSystemSuccess) = 1 - .00006912 = .99993088$$

$$P(RouterSystemSuccess) = 1 - .0000010 = .999999$$

$$P(WANSystemSuccess) = 1 - .0000090 = .999991$$

Therefore, using Equation 5.6, the average availability of the entire information system with crossover/fail-over points is:

$$A_{av(System)} = .99993088 * .999999 * .999991 = .99992088$$

This availability results in an average downtime of:

$$DownTime = \frac{41.5851 Minutes}{year} = \frac{.693085 hours}{year}$$

c. Availability Analysis

Using the same method of calculation as described in the above examples, the availability or downtime for a single Windows NT server system, a single Unix server

system, and a combination of multiple server systems were calculated and are displayed in Table 5.4 below.

Table 5.4: Summary of Average Downtime per Year

Platform(s)	Downtime per year (Minutes)	Downtime per year (Hours)
Single NT Server	15,505.2	258.42
Single UNIX Server	3,521.52	58.69
Two NT Servers	349.708	5.8285
NT-Unix Server Mix	41.5851	.693085
Two Unix Servers	9.0876	.15146

What is important about these numbers is that diverse and redundant systems can greatly increase system availability—but this is no surprise as the United States Navy has known this for a long time. The United States Navy has long ago learned to use diverse and redundant systems for navigation, propulsion, and other "mission critical" systems. For example, if the Navy were to loose tracking with the Global Positioning System (GPS) satellites in time of war, it would still have its diverse and redundant inertial navigation systems as a backup. If the Navy looses its single standard operating system (Windows NT 4.0/2000) to a virus, its Intel processor to some bug, comes upon some other denial of service attack, or meets some common cause equipment failure, the author is concerned that there will be nothing left to use as a backup to continue normal operations.

This availability, or unavailability depending on how one views it, could also result in increased costs to the United States Navy. According to Forrester Research Inc., downtime is costing major Internet players an estimated $8,000 per hour so far in 1999. (Sliwa, 1999) While the private sector does not exactly translate to the military, these figures are offered to give the reader an appreciation for the costs associated with downtime. Using the Summary of Average Downtime per Year from Table 5.4, and the

survey data from Forrester Research Inc., the costs for downtime is given in Table 5.5 below.

Table 5.5: Cost of Downtime per Year

Platform(s)	Downtime per year (Minutes)	Cost of Downtime per year
Single NT Server	15,505.2	$2,067,360
Single UNIX Server	3,521.52	$469,536
Two NT Servers	349.708	$46,628
NT-Unix Server Mix	41.5851	$5,545
Two Unix Servers	9.0876	$1,212

To get the biggest bang for the availability buck, and reap the benefits of a system void of common cause failures, in the author's opinion, the Windows NT-Unix combination is the best choice. It takes two Windows NT servers to get close to the availability of any other platform, but that would not even take into consideration the reduction of common cause failures. Furthermore, it does not even get close to the NVI IPT requirement of four nines, or an average of 0.876 hours of downtime per year. Finally, the numbers for the Windows NT-Windows NT and Unix-Unix combinations are overly optimistic of the average availability that could be obtained because they do not take common cause failures or single points of failure into account.

F. MITIGATING THE RISKS OF A SINGLE VENDOR STANDARD

So what can the United States Navy do to reduce the effects of common cause failures, or single points of failure, in its information system architecture? While the most important defense against accidental failures is redundant systems, they do not solve the entire problem. If the redundant systems are comprised of the same operating system, have the same hardware manufacturer, or if some other facet is in common, they can all be taken out by a common cause and the true benefits of a fault tolerant system will not

be realized. General defensive tactics to avoid common cause failures are described in Hoyland and Rausand's (1994) book, *System Reliability Theory.* Some of the more effective tactics include redundancy, monitoring, and diversity:

> ***Redundancy*** -- This is a tactic to improve system availability, but, by definition, common cause failures decrease the positive impact of this particular tactic. Nevertheless, increased redundancy will generally still have value.
>
> ***Monitoring, Surveillance Testing, And Inspection*** -- Monitoring via alarms, frequent tests, and/or inspections so that unannounced failures from any detectable causes are not allowed to accumulate.
>
> ***Diversity*** -- The mixture of interchangeable components made by different manufacturers (equipment diversity) or the introduction of a totally redundant system with an entirely different principle of operation (functional diversity) for the express purpose of reducing the likelihood of a total loss of function that might occur because all like components are vulnerable to the same cause(s) of failure. (Hoyland and Rausand, 1994)

It is through tactics and policy using redundancy, diversity, and monitoring (to name a few), where the author believes the Navy can increase and protect the availability of its information systems.

G. CHAPTER SUMMARY

When making strategic information system acquisition policy, all areas should be considered and costs should be given to all risks—including those of security. As Gartner Group analyst Fitzpatrick (1998) notes,

> While much attention has been paid to the total cost of operation (TCO) of user desktop appliances, little regard is given to the availability aspect of the back-end devices that are truly running the business. Only a handful of user organizations to date have taken even an initial stab at the cost to the organization of unavailability. System availability is key to success in the emerging global, electronic marketplaces. The future is 24X7 for most firms." (Fitzpatrick, 29 October 1998)

The military is no exception. In fact, the United States Navy, more so than commercial enterprise, relies on its equipment to correctly operate and be available 24 hours a day, seven days a week—365 days a year. If that equipment is not available, the United States Navy doesn't just loose money (as with private enterprise), but the possibility exists that they can loose the lives of sailors and soldiers.

If the military had already standardized on the single operating system/single PC standard, Operation "Desert Fox" (where United States forces conducted air attacks against Iraq for failing to comply with United Nations weapons inspectors) might not have been so successful. The 70 hour operation, that ended December 9, 1998, and reportedly used more Tomahawk cruise missiles than was expended during the entire Gulf War, would have resulted in an average Windows NT server downtime of more than two hours. Does two hours out of 70 sound like a lot? Maybe not, unless those were the two hours you needed to fire weapons to defend yourself from scud missile attacks.

When designing the Navy information system architecture, it is helpful to consider that redundant components do no good if they are subject to a common source of failure. Two replicated computer systems in the same room do not increase availability in the event of a fire, and having computer systems with the same operating system do not increase availability during a denial of service attack. It is easy to forget all the times that a system crashes because the individual events are usually short lived (the machine may be down for less than five minutes). "Given this, it is human nature to forget the little bumps when it comes time to acquire additional capacities, make platforming decisions, or set strategic direction." (Fitzpatrick, 1998) In the author's opinion, the United States Navy should look at these availability numbers when setting platform and operating system purchasing policy in the future.

Microsoft is well aware of their availability problems, and as Microsoft Corp. President Steve Ballmer said at a Networld+Interop conference in October 1998. "It will

be years before the PC can rival the mainframe in this area [availability]...One user I talked to had to reboot every four weeks because if they didn't, the server would crash." ("PC Week," 1998) If the Navy continues to move all Navy computing functions to a Windows NT-based PC, the author believes the Navy should exercise caution when including mission critical systems in that mix. If the five minutes that is needed to have the propulsion system get the ship out of harms way, is the five minutes that it takes to reboot the computer system, and it happens on a frequent enough basis, it can keep us from getting from point A to point B and endanger the lives of the sailors and soldiers on board Navy ships. "Given that approximately 80 percent of unplanned downtime is due to operator error and application failure, enterprises should focus increased investment in IT processes to improve availability and not rely chiefly on technology investments." (Scott, McGuckin, Claunch, 1998) No standard is going to be the "silver bullet" for the Navy's interoperability and fiscal woes. Even the recommendations contained in this thesis are but a snapshot in time and will also not provide that "silver bullet." In the author's opinion, the Navy should not standardize on a single vendor-based standard, but should instead, rely more on an 80/20-type rule. Standardize on 80 percent and use the 20 percent as crossover/fail-over so that single points of failure can be reduced. The 80/20 rule will still allow for economies of scale, but most importantly, it will allow the right tool to be used for the right job. In the author's opinion, the 20 percent of the applications where Windows NT will not work, the Navy shouldn't force it to work. The Navy should use another operating system or platform that is adequate for the task. Not only will this ensure that the best equipment is being used for the best job, but it will help eliminate common cause failures in the Navy information system architecture.

VI. IT-21 PROCUREMENT ISSUES

A. INTRODUCTION

The Armed Services Procurement Act of 1947, the Federal Property and Administrative Services Act of 1949, and the Competition in Contracting Act of 1984 have been used throughout history to govern and regulate federal procurements. More recently, the Federal Acquisition Streamlining Act of 1994 and the Federal Acquisition Reform Act of 1996, have been used to help streamline the acquisition process. These statutes have allowed the Government to procure items in a more economical and timely manner, have switched the focus from the use of military specifications to the use of commercial products whenever practical, and have redefined the purchase of information technology equipment as an investment vice a commodity. More specifically, the *Information Technology Management Reform Act (ITMRA)*, which was subsequently re-titled the *Clinger-Cohen Act of 1996,* required the Secretary of Defense to,

> ...develop...a process for analyzing, tracking, and evaluating the risks and results of all major capital investments made by an executive agency for information systems. The process shall cover the life of each system and shall include explicit criteria for analyzing the projected and actual costs, benefits, and risks associated with the investments. (ITMRA, 1996)

These requirements were initiated to help reduce the overall lifecycle costs the government pays for IT equipment, software, and services, and to help reduce the risks associated with purchasing information systems.

Whenever the Department of Defense, or any other Government agency, undertakes a new policy requiring the procurement of items to support that policy, it will most likely be subject to the statutes enumerated above and the Federal Acquisition Regulations. The Federal Acquisition Regulations, or FAR as they are more commonly referred, provide the basic set of regulations, policies, and procedures for the

procurement of supplies and services by the federal Government. When the United States Navy introduces any new information system acquisition policy, that policy also becomes subject to these laws and all their provisos.

One of the main premises and underlying themes of all these statutes is that of competition. This chapter will explore the competitive requirements contained in these statutes and the Federal Acquisition Regulations. In addition, a case study will be introduced detailing the procurement problems associated with the selection of a single vendor-based standard. Finally, recent Department of Defense procurement practices will be explored to bring attention to the jeopardy associated with the potential failure of the United States Navy to comply with the FAR and other applicable procurement laws.

B. COMPETITION

Congress has a long history of requiring competition in the procurement of Government items, equipment, and services. One of the first laws enacted to require competition in federal procurements was ratified in 1809. More recently, the Competition in Contracting Act (CICA) was passed which made "full and open" competition the principal objective in Government procurement and it imposed strict limits on the use of "sole source" procurements. Many of these laws requiring competition are found in the United States Code. *Title 10 of the United States Code Section 2304* states that, "... except in the case of procurement procedures otherwise expressly authorized by statute, the head of an agency in conducting a procurement for property or service," in this case, the Department of Defense, "...shall obtain full and open competition through the use of competitive procedures in accordance with the requirements of this chapter and the Federal Acquisition Regulations..." It is often not clear whether a particular information system acquisition policy provides for full and open competition. In the author's opinion, the adoption of a single vendor standard does not provide for full and open competition. However, the law is filled with exceptions to

the full and open competition regulations, making it difficult to determine the status of the policy. These exceptions will be explored to determine if any apply to the United States Navy and if the Navy information system acquisition policy is in concert with the history of competition required in federal procurements.

1. Full and Open Competition

The various titles and sections of the United States Code enumerated above provide the foundation and framework for what are the Federal Acquisition Regulations (FAR). The Federal Acquisition Regulations are applicable to the Department of Defense, NASA, and other government agencies, and they describe, among other things, the requirements for the effective-use of competition in DOD acquisition policy. In particular, Federal Acquisition Regulation Part Six (FAR Part 6) describes the policies and procedures used to promote full and open competition in the acquisition process. These regulations and laws were not put into place to be restrictive or counterproductive. Their purpose is to help ensure the government makes fair and frugal acquisitions of commercial products and services. Competition is important because, as most economists agree, it will lower the costs of the process of procuring and equipping military forces with, among other things, information technology products and services. As such, it is the author's belief that these regulations should be seen as beneficial to the Department of Defense and followed to the greatest extent practical.

To better understand the rules regarding competition, Part Six of the Federal Acquisition Regulations will be examined to determine if the Navy policy complies with the "full and open competition" requirements stated in the regulation. "Full and open competition,..." as defined by the FAR Part 6 Competition Requirements, means that, "...all responsible sources are permitted to compete." With the selection of a single vendor standard, in the author's opinion, no other companies are permitted to compete, and as such, it would not provide for "full and open competition."

The relationship that exists with a vendor-based information system acquisition policy more closely follows that of a "Sole Source acquisition." FAR Part 6 defines a sole source acquisition as, "...the purchase of supplies or services that is entered into or proposed to be entered into by an agency after soliciting and negotiating with only one source." The selection of Microsoft Windows NT as the sole Network Operating System, the selection of Microsoft Exchange as the sole email solution, and the selection of Microsoft Office Professional as the sole Office Automated System Software for the United States Navy IT-21 standard, falls in line with the concept of a "sole source acquisition." The question now becomes, is the Navy allowed to perform a sole source acquisition, and/or are there any exceptions to the full and open competition rules that would allow the Navy to use a single vendor for its information technology standard?

2. Exceptions to Full and Open Competition

Under the Federal Acquisition Regulations, full and open competition shall be promoted and provided for by contracting officers except under certain limited exceptions. These exceptions fall into two main categories: (1) full and open competition after the exclusion of sources, and (2) other than full and open competition.

In the first category, one or more sources may be excluded from consideration before full and open competition is provided, but only under certain circumstances. Under full and open competition after the exclusion of sources, the Department of Defense "...may exclude a particular source from a contract action in order to establish or maintain an alternative source or sources for the supplies or services being acquired..." (FAR 6, 1999) After the exclusion of the source, full and open competition must be used with the remaining sources. In the author's opinion, this particular exclusion does not pertain to the single vendor standard as there are no alternative sources for the supplies or services being acquired—Microsoft is the only source. This leaves the "other than full

and open" competition category as the final avenue for determining the congruency of a single vendor-based standard with federal procurement competition requirements.

Title 10 of the United States Code Section 2304(c), details when the Department of Defense may use other than full and open competitive procedures. As a matter of policy, contracting without providing for full and open competition is a violation of 10 USC 2304 and the FAR unless permitted by one of the following exceptions. Full and open competition need not be provided for,...

- When the supplies or services required by the DOD are available from only one or a limited number of responsible sources, and no other type of supplies or services will satisfy agency requirements.
- When the agency's need for the supplies or services is of such an unusual and compelling urgency that the Government would be seriously injured unless the agency is permitted to limit the number of sources from which it solicits bids or proposals.
- When it is necessary to award the contract to a particular source or sources in order to achieve industrial mobilization; to establish or maintain an essential engineering, research, or development capability; or to acquire the services of an expert or neutral person for any current or anticipated litigation or dispute.
- When precluded by the terms of an international agreement or a treaty between the United States and a foreign government or international organization, or the written directions of a foreign government reimbursing the agency for the cost of the acquisition of the supplies or services for such government.
- When authorized or required by statute.
- When the disclosure of the agency's needs would compromise the national security unless the agency is permitted to limit the number of sources from which it solicits bids or proposals.
- When the agency head determines that it is not in the public interest in the particular acquisition concerned. (FAR 6, 1999)

3. Brand Name/Sole Source Procurements

Of the above exceptions, only one exception in the author's opinion, applies to the single vendor standard. That exception would be the first, only one responsible source and no other supplies or services will satisfy agency requirements. The FAR describes

the application of this regulation for brand name descriptions. The exception reads, "An acquisition that uses a brand name description or other purchase description to specify a particular brand name, product, or feature of a product, peculiar to one manufacturer does not provide for full and open competition regardless of the number of sources solicited." (FAR Part 6) From the reading of this sentence, it would appear that acquisitions that use brand name descriptions never provide for full and open competition, and this is probably true in all reality, but that doesn't necessarily prohibit the use of brand name descriptions.

When this exception is exercised in the procurement process, it eventually takes the form of a "sealed bid" or "competitive negotiation." When a "sealed bid" procurement describes a product to be furnished by a brand name or its equal in order to be responsive, the Government must proclaim the salient characteristics of the product. These salient characteristics are the most significant physical, functional, or other characteristics needed to be present in order for the bid to be responsive. "To ensure as much competition as possible under the circumstances, all known commercial items that will serve the Government's purposes should be listed as acceptable *brand names.*" (Arnavas and Ruberry, 1994) This would allow vendors of other products who meet the salient characteristics described by the Government to be listed as a brand name product or its equal. But as Arnavas and Ruberry describe in the second edition of their *Government Contract Guidebook (1994),* "*Brand name or equal* specifications are not particularly encouraged since they can cause misunderstanding, confusion, and protest. As a result, they should be used only when no other specification is available."

Competitive negotiation procurements require the same elements of full and open competition as sealed bid procurements, except in the case of sole-source procurements. However, "...if the procurement must be conducted on a sole-source basis, the Contracting Officer must justify this requirement and take steps, whenever possible, to avoid resort to subsequent noncompetitive procurements." (Arnavas and Ruberry, 1994)

As a result, a non-competitive procurement may occur if it is "...justified and approved in accordance with FAR 6.303 and 6.304. The justification should indicate that the use of such descriptions in the acquisition is essential to the Government's requirements, thereby precluding consideration of a product manufactured by another company." (FAR Part 6) So now that it has been determined that, with the proper justification, full and open competition is not required for brand name or sole-source acquisitions, it must be determined whether or not the proper justification exists for a vendor-based sole source acquisition.

4. Sole Source Acquisition Justification

As a requirement for the justification of a sole source contract, the contracting officer must justify the use of such actions in writing, certify the accuracy and completeness of the justification, and obtain the necessary approval for the justification. This approval is required at differing levels of the Department of Defense depending on the dollar amounts of the acquisition. In this case however, the approval is not of concern. The concern is the justification of the acquisition. These justifications must be certified to be complete and accurate by the technical or requirements personnel responsible for that data, and these justifications and any other related data, must be made available to the public under the provisions of the Freedom of Information Act.

a. Specifications

Whenever a "need" of the Government is identified and then filled through the procurement of commercial products or services, those needs are defined through Government specifications. The FAR defines a specification as "a description of the technical requirements for a material, product, or service that includes the criteria for determining whether these requirements are met." (Arnavas and Ruberry, 1994) These specifications can not be legally or ethically crafted to steer the procurement in the

direction desired by a particular Government agency. In fact, the law requires that the head of an agency shall "...develop specifications in such manner as is necessary to obtain full and open competition...and include restrictive provisions or conditions only to the extent necessary to satisfy the needs of the agency or as authorized by law." (Arnavas and Ruberry, 1994) Furthermore, the FAR states that a specification, "...shall state only the Government's actual minimum needs and be designed to promote full and open competition, with due regard to the nature of the supplies or services to be acquired." (Arnavas and Ruberry, 1994) The key phrase of "minimum needs" is important because it helps promote full and open competition by ensuring the specifications are not unduly restrictive. As Arnavas and Ruberry (1994) proclaim, "A specification that exceeds the Government's minimum needs by containing unnecessary requirements improperly restricts competition since it may prevent one or more bidders from submitting responsive bids." This puts the Government in a very difficult position. They have to be specific enough to meet their "minimum needs," but not overly precise as to prohibit competition. If multiple Network Operating Systems will meet the United States Navy minimum needs, then it makes it more difficult for the Government to justify a sole source single vendor-based procurement.

5. Would Another NOS Meet the Navy's Minimum Needs?

The ITSG is not far from the IT-21 policy, but it does have some minor differences. For example, while Windows NT is still the recommended operating system, there is room for other operating systems when it is not practical to use NT. While this may seem like a subtle difference, it is an important difference in the author's opinion. It takes into consideration the end users' needs by allowing a system other than a mandatory "standard," to be used in the Navy information system architecture when the Windows NT standard is not practical to use. As the ITSG states, "When Windows NT is not practical, use operating systems that are standards based, primarily those that comply

with TOG's X/Open CAE and...POSIX specifications. Operating systems should be multitasking and multithreaded and enable parallel processing." (ITSG) Table 6.1 below shows the ITSG recommended network operating systems.

Table 6.1: Recommended Implementations for Server Operating Systems

Expiring ITSG	Current ITSG	Projected ITSG			Potential ITSG
Not Recommended	1998	1999	2000/2001	2002/2003	Emerging
NetWare 3.x or less Vines	Windows NT Server Unix 95 (X/Open CAE) POSIX NetWare 4.1 or later	Windows NT Server Unix 95 (X/Open CAE) POSIX NetWare 4.1 or later	Windows NT Server Unix 95 (X/Open CAE) POSIX NetWare 4.1 or later	Windows NT Server Unix 95 (X/Open CAE) POSIX	Microkernel OSs
Activities, Platforms, Operational Environments	All				

From ITSG, 1998.

If these other network operating systems also meet the "minimum needs" of the Navy, then it makes it more difficult for the Government to justify a sole source acquisition. It also does not take full advantage of the competition involved with other types of acquisitions, and therefore, does not benefit from the increased competition and lower costs that these other procurements often obtain.

C. CASE STUDY: OPERATING SYSTEM/COMPUTER PLATFORM STANDARDIZATION AT NASA

When trying to ascertain the optimal course of action in a particular situation, it is often helpful to investigate similar situations to determine the lessons learned and how to better proceed in the future. When trying to determine the course of action the Navy should take in the next version of its standardization policy, it is also helpful to examine like situations. While every case should be judged on its own merits, other situations

similar to the Navy's own may help determine the optimal course of action in a specific case. While the specific operating systems and computer platforms in the case study at the National Aeronautics and Space Administration (NASA) are not important and have now since changed, it is the general ideas permeating this case, and the controversy and outcome of the selection of a single vendor-based standard, that will be explored. In the author's opinion, it is important to examine this case in order to help the United States Navy benefit from the "full and open competition" requirements of the law, and to prevent the threat of protest or a Congressional investigation into United States Navy information technology acquisition policies.

1. Specifics of the Case

In 1995, the Chief Information Officer (CIO) at NASA's Johnson Space Center (JSC) declared Microsoft Windows 95 as the standard desktop operating system. This vendor-based operating system standardization at NASA provided the rationale for the replacement of almost all Macintosh workstations at the Johnson Space Center. This policy met opposition within NASA at the "end user" level. These users at JSC complained that the policy was "...intended to specifically eliminate all Macintosh microcomputers at JSC, was not cost effective, and could have a detrimental effect on NASA's space flight mission." (NASA OIG, 1996) The users compiled data to make their case.

As a part of their case, these users disclosed the fact that "help desk" calls increased from 68,000 in 1994 (pre-Windows standardization) to 142,000 in 1996 (post-Windows standardization)—an increase of some 209 percent. It was also shown, through a number of in-house studies, market studies, and a study performed by the Gartner Group, that the Macintosh platform was the more cost effective platform—taking into consideration the full range of life-cycle support costs. As such, it appeared to the end user that they were being forced to accept a lesser quality and capability platform and

operating system than was previously available. They also felt that the policy was not just anti-Macintosh, but was pro-Microsoft.

These feelings were not just being shared by the end users at the Johnson Space Center, but they were being embraced by other competitors in the commercial market as well. In August of 1996, Novell wrote a letter to the NASA Office of the Inspector General stating, "It is becoming more apparent that a unilateral decision [selecting Exchange and NT] without the merit of sound technical and procurement specifications and with undue bias towards a single vendor [Microsoft] has been made and implemented within NASA."("Takeover at NASA," 1998) What was Novell's basis for such a statement? Well, Novell requested the requirements documents of the products selected at NASA and the studies supporting the selection of those products. "Novell never received these documents and were later told these documents never existed. These documents supporting the selection of NT and Exchange do not exist, but documents which do not support the selection do! Obviously, this presented a problem with Novell. Not only was there a possible bias at JSC, but also within NASA as a whole..." ("Takeover at NASA", 1998) The end users at NASA and other market competitors then forwarded this data to the NASA Chief Information Officer, the NASA Office of the Inspector General, and to their Congressmen.

2. Congressional Reaction

Upon receiving this complaint, the NASA CIO clarified NASA's policy on the acquisition and management of information technology in June of 1996 when he said,

> In general, we must examine the rationale for each such decision to ensure that it is consistent with Agency policy and that any [IT] decision which restricts full and open competition is both necessary and justified. More specifically, this letter clarifies our interoperability standards and the role of competition in achieving this objective.

> Regarding our interoperability standards strategy, the Agency consciously decided that it was in our best interest not to establish a single desktop computer operating standard. Rather, we endorsed an IT architecture which supported multiple desktop operating systems. Quite simply, we recognized that the diversity of our end-users' requirements and applications necessitate that our IT architecture be flexible enough to adapt to and optimize their needs. (NASA OIG)

However, the upper-level management of NASA was saying one thing yet doing another. They continued to standardize on a single-vendor desktop operating system standard—Windows 95.

Congress then held hearings to determine if NASA was violating the full and open competition requirements of the FAR and other applicable laws and regulations. In a 1997 article published in *Federal Computer Week*, Harreld (1997) quoted a draft of a House of Representatives letter that characterized the switch to PCs at NASA as possibly "in violation of your legal obligation to ensure fair and open competition in your procurement practices." (Harreld, 1997) This House letter, which was to be delivered to the NASA Administrator, was to instruct "Goldin [NASA administrator] to assess the policy and ensure that Garman [JSC CIO] is adhering to federal procurement policies that allow fair and open competition in the acquisition of information technology." (Harreld, 1997) NASA's deputy associate administrator for procurement, Tom Luedtke, responded by saying, "NASA crafts all procurements to ensure fair and open competition. 'If there is a legitimate need to have one particular system, and we know there's only one company that makes that system, it may be a sole source.'" (Harreld, 1997) While this statement is true, the proper steps to justify that sole source acquisition must be undertaken to help ensure competition is maintained in the federal procurement process.

3. NASA Office of Inspector General Conclusions

In November of 1996, the National Aeronautics and Space Administration, Office of Inspector General, Inspections and Assessments Branch, released a report titled, *Johnson Space Center Information Technology Equipment Replacement,* to address the issues surrounding the replacement of computing equipment and the standardization on a single vendor computing solution at NASA. In that report, the NASA Inspector General concluded that:

- The policy decision and its implementation was not in conformance with the stated NASA CIO policies,
- The policy decision was not cost effective and no cost/benefit or life-cycle cost analyses was conducted to support the replacement acquisitions,
- JSC did not conduct information technology (IT) acquisitions with regard to users' requirements, and
- Potential exists for a negative impact on space flight mission and safety. (NASA OIG, 1996)

The second element of the IGs conclusion is an important one because it is this type of analysis that is required to justify a sole source award. When the IG discussed this lack of documentation with the responsible Contracting Officer, "The Contracting Officer could not confirm that the studies had been performed." (NASA OIG, 1996) In trying to support their claim for a single-vendor operating system standard, the NASA CIO said, "We are confident we are going to save money." ("Takeover at NASA," 1998) The law requires more than a hunch to justify a sole source acquisition. As a result, the IG conducted its own life-cycle analysis and came to a very different conclusion. The results of their analysis are detailed in Table 6.2 below.

Table 6.2: 5-Year Cost of Ownership
Windows 95 vs. Macintosh OS 7.5

Number of Platforms	Windows 95	Macintosh OS 7.5	Difference
1 Computer	$35,859	$35,124	$735
3,500 Computers	$125,506,500	$122,934,000	$2,572,500

From NASA OIG, 1996.

The NASA IG determined that the estimated 5-year cost of ownership was approximately $735 more per desktop with the purchase of Windows 95 desktop workstations. Based on these numbers, the acquisition of 3,500 Windows 95 workstations, required to implement a vendor based desktop operating system standard, would be more expensive to the tune of $2,572,500 dollars. These costs didn't even include the migration costs (software conversion costs, acquisition of replacement software costs, training costs, etc.) from one platform to another, which was estimated at $2,900,000 dollars. In the author's opinion, the Navy should learn from NASA's mistake and make sure it bases its acquisition policy on the facts and numbers vice a hunch that, "...we know we will save money." If the Navy does this, they should be able to prevent this type of scrutiny over their acquisition policies in the future.

4. Outcome of the Case

As a result of the information presented by the end users and the resulting NASA OIG inspection, the following recommendations were submitted to the NASA and JSC management:

- Take action to comply with NASA CIO and Federal Information Resource Management published policy, guidelines, and standards. The NASA CIO...and the Office of Procurement should take steps to review JSC compliance and assure necessary corrective actions are taken.

- Conduct comprehensive requirements analyses to identify end-user information technology (IT) needs.
- Perform cost-benefit and life-cycle cost analyses to include replacement software acquisition and/or conversion costs and anticipated training costs prior to initiating major IT acquisitions for desktop workstations.
- Evaluate the impact on space flight mission effectiveness and safety prior to replacement of currently installed equipment and software. (NASA OIG)

When conducting procurements or establishing new IT policies for the United States Navy, the author believes the Navy should follow, among other things, the same recommendations enumerated above. For the Government to reap the benefits of a competitive procurement environment, it needs to ensure it adequately justifies all "sole source" acquisitions. Without this justification, the United States Navy will expose itself to bid protest and slow down a procurement process that already travels at a snails pace.

D. RECENT DOD ACQUISITION PRACTICES

The Department of Defense, Office of the Inspector General released a report in March of 1999 detailing some recent procurement practices that could be of concern in future Government acquisitions. According to the report, "Defense Department contracting officials have engaged in 'questionable' procurement practices, costing taxpayers millions of dollars in higher prices and denying some vendors a fair opportunity to be considered for DOD contracts...In the worst cases, technical evaluators were able to technically 'disqualify' contractors before cost was even considered." (Verton, "IG", 1999) In the author's opinion, there is apparently a small percentage of contracting offices that "steer" contracts, have their own procurement agenda, or just lack the training to ensure the procurement laws are faithfully executed. As the report affirms,

> Contracting officials throughout DOD also "routinely" relied on "questionable" technical evaluations to award task orders without regard to price differences,...In fact, in one instance an Air Force contracting official made an award to a contractor whose price was 134 percent higher

> than another offer, causing an internal legal reviewer to call for a "sanity check" on the process...The report also identified a Navy contracting office that selected a "preferred" contractor without performing a cost/technical trade-off analysis. (Verton, "IG", 1999)

While a number of the procedures for the procurement of commercial products and services by the Government are cumbersome and time consuming, it is the author's belief that they are a necessary element in the conservation and promotion of full and open competition in the procurement process. However, not all of these procedures are being accomplished. The DOD IG report found that contracting officers awarded 66 of 124 task orders on a sole-source basis without adequate justification. This information is graphically depicted in Figure 6.1 below.

Figure 6.1: Sole-Source Task Order Awards

After DOD OIG, 1999.

This inadequate justification denied, "...other contractors a fair opportunity to be considered." (DOD OIG, 1999) The total value of these contracts was $87.6 million dollars. If 53 percent are not adequately justified, then another vendor may have been

able to provide an acceptable alternative product or service at a decreased price, thus saving the Government millions of dollars.

What remedies are available to the vendors who did not get these contracts? Relief is primarily achieved through bid protest. However, these companies make a business decision on whether or not they think they can win, the legal costs to prepare the protest, and what that protest will do to their reputation and chance of obtaining future government business. In many cases, no protest is offered. Furthermore, as the DOD IG audit uncovered, "...we encountered discouraged vendors who were afraid to challenge prospective awards because of concern about future dealings with the same contracting officer and program office." (DOD OIG, 1999)

As a result of these problems, the IG recommended that the Under Secretary of Defense for Acquisition and Technology, "...take several actions to increase competition in the award of task orders for services under multiple award contracts. Because of reported problems for this area, the Office of Federal Procurement Policy has issued guidance recently to stop program offices from designating preferred vendors and set a goal that 90 percent of the task orders should be competitive." (DOD OIG, 1999) While it is legal to issue orders under multiple-award contracts without competition, the IG concluded that, "...we believe it is not in the best interest of DOD that price consideration in task orders has become the exception rather than the rule." (Verton, "IG", 1999)

Finally, the report detailed a situation where DOD officials allowed one contractor to be the sole provider of services for over 9 years without competition. After the issuance of the IG audit, the agency awarded the contract on a competitive basis. As a result, the agency realized a 40 percent decline in the hourly rates for the contracted services from the prior sole-source contract. (DOD OIG, 1999) While the sole source contract seemed to be in the interest of the Government each time it was awarded to the

same provider, and it was probably more expedient, it was also more expensive. When conducting IT procurements for the United States Navy, it is the author's opinion that the Navy should try to avoid the use of these type of questionable practices to help ensure the Navy gets the best products at the best prices. If the Navy does not take these cost factors into consideration, it will likely end up paying a lot more money than is necessary to implement the Information Technology for the 21st Century policy and whatever policy follows IT-21.

E. CHAPTER SUMMARY

The Information Technology Standards Guidance (1998) states that its standards, "...must be properly used in the acquisition process. They cannot be used as justification for less than full and open competitive acquisition. Purchasing agents and contracting officers continue to be responsible for appropriate source selection and price reasonable decisions." (DON CIO ITSG, 1998) The job of the Government in providing a full and open competitive acquisition environment is difficult. However, the Government must find a balance between setting specifications that are detailed enough to meet the Governments needs yet not overly specific as to prevent competition. In the author's opinion, the selection of a single vendor-based standard seems to run counter to the spirit of competition required in the federal acquisition process. However, the legality of the policy boils down to the justification provided for the issuance of the contract, and as Arnavas and Ruberry proclaim, "In the absence of clear and convincing evidence that the agency's judgement is unreasonable, an agency's determination of the Government's minimum needs and the best method of obtaining those needs will not be overturned." (Arnavas and Ruberry, 1994) This gives the Navy great latitude in the procurement process. In the author's opinion, the Navy should not abuse that latitude, but take advantage of the benefits that competition provides. By establishing a vendor-based standard, that standard could create an anti-competitive climate with the potential to

create sub-optimal information systems as a matter of both function and cost. It is this type of concern that should be addressed in the follow-on to the IT-21 standardization policy.

VII. THE PRACTICAL ISSUES OF IT-21

A. INTRODUCTION

The *Information Technology for the 21st Century* policy requires all non-standard Network Operating Systems (NOS) and email products to be replaced no later than December of 1999. The policy names Windows NT Server version 4.0 as the standard fleet NOS, Microsoft Exchange version 5.0 as the standard e-mail solution, and Microsoft Office Professional 97 as the standard fleet Office Automation System software. These standards were formulated and then promulgated through a Commander in Chief, United States Pacific Fleet (CINCPACFLT) and a Commander in Chief, United States Atlantic Fleet (CINCLANTFLT) supported message to help reduce the costs of operating United States Navy Information Systems (IS) and to help increase fleet-wide interoperability.

However, in the author's opinion, reduced costs are not necessarily provided through the selection of a single vendor-based standard. Reduced costs and increased functionality are provided through the ability to purchase "best of breed" products in a *competitive* environment. Furthermore, it is the author's opinion that interoperability is not guaranteed with the selection of a single vendor standard. While interoperability problems may be reduced somewhat with the selection of a vendor-based standard, they will probably not be eliminated. In addition, interoperability can be achieved with multiple products and multiple vendors if the right management philosophy and information systems architecture are developed and implemented. In the author's opinion, this management philosophy and architecture should help keep the vendor-based standards the United States Navy picks today from becoming the legacy systems of tomorrow.

The United States Navy should concentrate on standardizing the interfaces of their information systems vice standardizing on vendor-based software applications or

operating systems if it wants to provide fleet-wide interoperability. As Emmett Paige Jr., former Assistant Secretary of Defense for C3I argued,

> We have been burned in the past by the acquisition of vendor proprietary systems that represented the best value for the money at the time, but whose upgrades proved too costly as time and technology advanced. We have learned our lesson—standardize the interfaces, using commercial standards whenever possible to create a systems environment in which individual creativity can flourish, so the component software (and hardware) systems can rapidly evolve and be integrated into a stable matrix of interoperable systems at minimum cost and downtime. ("Applying COTS," 1999)

A computer application is not an interface as it relates to the transfer of information produced by that product, and as a result, the standardization on a particular vendor-based application will not necessarily provide interoperability. The format that the file is saved in provides the interface for its transfer, and it is that interface that will provide for increased interoperability. For example, if two different word processing programs save a file in the same format, then they will most likely be interoperable. The file will be usable on both platforms using different word processing programs. As long as the interface, or format, is the same, then the documents will be interoperable. It is this interface, in the author's opinion, where the United States Navy should concentrate its standardization efforts.

This chapter will examine the practical aspects of the IT-21 policy to include the risks associated with commercial-off-the-shelf (COTS) software. Next, the risks of choosing a standard that must maintain coherency with previous versions of software will be explored. Through an examination of the practical application of a single vendor-based standard, a concept known as the "Lasagna Effect," and the lag time from standards adoption to implementation, it will become apparent why a single vendor-based standard will not necessarily eliminate the United States Navy interoperability woes. In addition, it will be shown how interoperability can be maintained without a single

vendor-based standard. Finally, the dual platform support cost "premium" myth will be revealed. Through a practical examination of these examples, several concerns associated with the Navy homogeneous vendor-based standard will be revealed in an attempt to identify areas of improvement for the standardization policy beyond IT-21.

B. PRACTICAL RISKS OF COMMERCIAL-OFF-THE-SHELF (COTS) PRODUCTS

With the ever-increasing financial constraints on the military, there has been a growing movement towards the purchase of Commercial-Off-The-Shelf (COTS) products to reduce costs and make the Navy's limited dollars purchase more vital information system resources. However, these COTS products have not been tested in battle conditions, and some COTS products are not adaptable to the military environment. "A growing band of COTS critics says forcing the military to accept commercial standards because Congress will not fund new technology R&D for the Pentagon will put US forces into the field with equipment that often does not meet real-world battlefield needs." (Wilson, 1999) In the author's opinion, the Navy should continue to exercise caution when employing COTS and use it where it make sense, and forgo its use when it does not. Dr. Mark Hartney of DARPA's Electronics Technology Office agreed when he said, "COTS won't meet all military requirements..." Take a display system for example. COTS displays do not have the, "...backlighting, wider operating temperature range, hermetic packaging, EMI (electromagnetic impulse) shielding, or odd sizes for retrofits,..." (Wilson, 1999) While this is a relatively simple example, it highlights the complexity involved in making the decision to purchase COTS products. In the author's opinion, the Navy should not just purchase COTS products because they are cheaper. The Navy should purchase COTS products because they meet the military requirements and it makes sense to use them in a particular situation.

The movement to push Windows NT into all aspects of the Navy, to include command and control, weapon systems, and propulsion systems, is disconcerting to the author. While one doesn't like to be on the receiving end of a "blue screen of death" (BSOD), the BSOD is a reality that happens with Windows NT. In the author's opinion, the Navy should be sensitive to the fact that computer crashes have different effects in different situations. If a computer crashes when a person is composing a word processing document, that person may get upset, but they can recover from their backup files with little to no damage to the final output. They can go get a cup of coffee while their system reboots and continue on with their day. If a computer crashes when it is providing a mission critical application, like that of a propulsion or weapon system on a ship, lives are now relying on that COTS software. Any sailor who has used COTS software would be less than ingenuous if they said they were comfortable with COTS reliability—so comfortable that they were willing to put their life in the hands of that COTS product. The business model for such products does not reward availability and reliability. Increased functionality and timeliness to market are the rewards, and these rewards often foster a culture complacent with the concept of software bugs. In the author's opinion, until this culture is changed and reliability becomes the reward, there will be too many bugs in some of these COTS software applications to put them in mission critical areas of the ship, or in other mission critical areas of the Navy information system architecture.

In a recent poll conducted by *PC World* and *World Research*, almost 80 percent of the 773 respondents said they had bought software that turned out to have bugs, and almost 50 percent of these respondents have lost data or files as a result of these bugs. Some 86 percent of the respondents believe the products contain bugs because companies rush their products to market before the bugs are worked out. (Spanbauer, 1999) By purchasing COTS software, the Navy is also subject to all these software bugs. However, if the Navy uses them in mission critical applications, the possibility exists that it will not

just lose data, but there exists the very real possibility that it could lose the lives of sailors and soldiers due to these bugs.

This distressing trend does not seem to be changing, and as software products get more complex, more and more bugs seem to rear their ugly head. The Internet seems to exacerbate this situation as some vendors attempt to cut corners on quality as they can easily post a patch to any bug in their software on the web. As Cem Kaner, a software development consultant, consumer advocate, and co-author of *Bad Software* claims, "As we ship products on Internet time, we're shipping them sooner and buggier,...We can fix things for free by putting the patches or service packs on our Web sites, so we don't have to test or fix as much before the first release." (Spanbauer, 1999) As a purchaser of COTS software, the United States Navy should come to terms with the fact that the software it buys will have bugs. As a result, it is the author's belief that the Navy should give careful consideration to deploying COTS software in mission critical areas of its infrastructure.

Furthermore, in some cases, a great deal of "value added" effort needs to be performed in order to meet the requirements of the Navy. "Logistics practices, parts replacement, component obsolescence, useful system life span, technology refreshment, packaging technology, performance requirements, power consumption, heat dissipation, environmental constraints, and electrical emissions are all technical and service related issues, any one of which can become a 'trigger' requirement which separates DOD requirements from the COTS market." ("Applying COTS," 1999) Figure 7.1 below displays this very requirement.

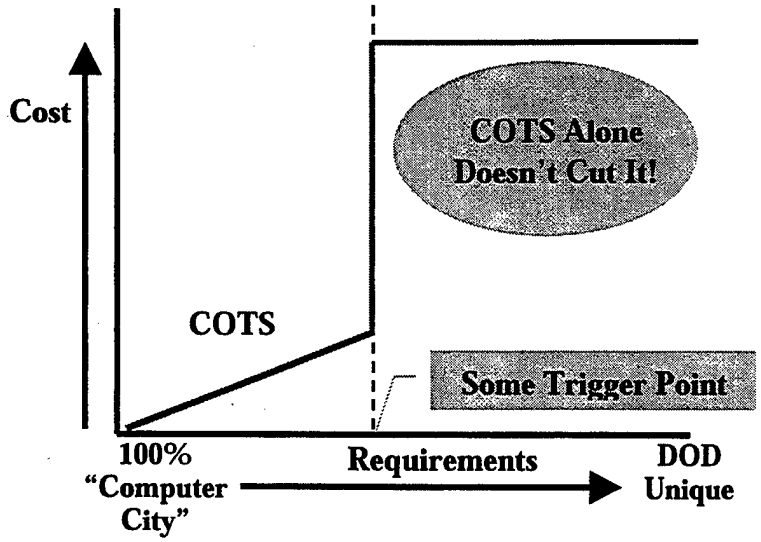

Figure 7.1: DOD Requirements "Trigger Point" for COTS

From "*Applying COTS*," 1999.

At some "trigger" point it no longer becomes as obvious that COTS is the cheaper way to proceed. At this "trigger" point, research should be conducted to insure that the value added components required to meet DOD requirements is not more costly than a government contracted and developed system. COTS is not always the best answer to the Navy's problems. As Larry Core, a project manager at the Naval Research and Development Center (NRAD) Tactical Advanced Computer Project Office noted, "There will always be places where COTS simply won't do...A paper map with a bullet hole is still a map—an electronic display of a map with a bullet hole is a brick." (Wilson, 1999) In the author's opinion, the Navy should not place over-reliance on high technology solutions and replace low-tech, or even no-tech, methods that have been verified in battle for generations, until at least, these high tech solutions can be shown to be reliable in battle. Unfortunately, they have to be used in battle in some capacity in order to determine if they will be reliable in battle. The author believes the Navy should use these

items in non-mission critical applications or maintain a "manual override" so the high technology solution can be scrapped if it is not working during battle.

C. THE COSTS OF MAINTAINING COHERENCY

When choosing a standard it is important to try to identify all the risks associated with that standard. While many view Microsoft as a "safe" choice for a standard, there are some risks inherent to Microsoft that many do not recognize nor factor into their decision making process. One of the risks associated with Microsoft, and other COTS vendors for that matter, is the requirement to maintain coherency with previous versions of their software. Figure 7.2 below displays the relationship of maintaining coherency with previous software versions and development costs.

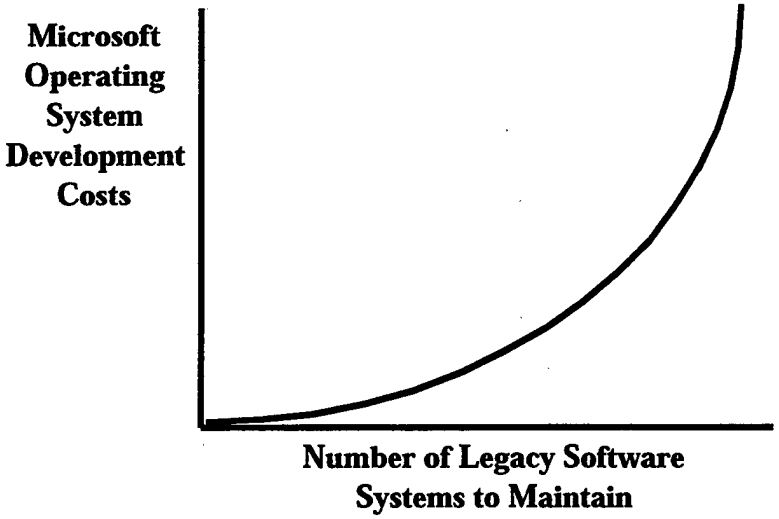

Figure 7.2: Costs of Maintaining Coherency with Previous Software Versions

If a vendor is able to maintain coherency with previous versions of their software, it will allow the customer the ability to use legacy software. However, there comes a point where this endeavor becomes cost prohibitive for the vendor. To maintain coherency, the vendor incurs added costs to test, migrate, and maintain that software. At

some point the vendor decides to leave the legacy behind so greater advances can be made to the functionality of their software. In their research note, *Constraints on Microsoft: The Hidden Factor*, Gartner Group analysts Hayward et. al. (1999) note,

> As the mismatch between choices incorporated in an architecture and its environment increases, the cost of creating new software that maintains architectural coherence with previous versions becomes excessive; i.e., an alternative source not subject to the same architectural constraints will offer better value. A dominant supplier can leverage its position to change the architectural rules, but when it does so, it concedes a key advantage: Architectural lock-in, the realization of that dominance, is lost. This is not a theoretical argument. As time passes, and Microsoft extends the scope of Windows, the impact of the architectural constraint becomes increasingly apparent. (Hayward, 1999)

The computer industry has seen ever-increasing examples of Microsoft's difficulty in this endeavor. In its attempt to maintain coherency with MS DOS and 16-bit applications, Microsoft built the NT Virtual DOS Machine (NTVDM) and the Win16 on Win32 (WOW) environment. The NTVDM and WOW provides a simulated MS-DOS environment for legacy MS-DOS-based applications and other 16-bit applications to run on Windows NT. However, this added functionality does not come without a price. The WOW environment does have some limitations. For example, if a Win16 application fails, it can prevent all other Win16 applications running in the same NTVDM from executing until the failed application is closed. In trying to maintain coherency with previous versions of their operating system, Microsoft was not able to provide preemptive multitasking within the NTVDM/WOW environment. Interoperability problems can also be encountered when Win16 applications do not follow the OLE and DDE specifications or if they rely on shared memory to exchange data. If this is the case with these programs, they will not function correctly in separate memory spaces and must be run in the default (shared) NTVDM and WOW application environment.

Another problem Microsoft is having with coherency involves the transition from Windows 95/98 to Windows 2000. The long delay in the release of software is often a result of trying to maintain this coherency. As Craig Beilinson, Microsoft product manager for Windows NT notes, "The upgrade to Windows 2000 Professional from Windows 95 or Windows 98 still has too many issues, so we're spending a lot of time working on that." (Gaudin "Beta 3", 1999) Most of these issues include the coherency required to migrate Windows 95/98 users to Windows 2000. As Beilinson notes,

> We have to figure out a way to bring your applications forward...If I install Windows 2000, and then I install Office or Notes or Word, that should work fine. But if I'm first on 95 and I've got my apps installed and then I upgrade to Windows 2000 on top of that, we're in a different place now. The application is already installed, so it doesn't know it's running on NT and has to run differently.

Beilinson said he isn't yet sure how Microsoft will solve that problem, but he hopes to have the solution in place before the final software release. (Gaudin "Win2000", 1999) In the author's opinion, the additional testing to maintain this coherency will make the upgrade to Windows 2000 more costly.

Windows 2000 has roughly 80 percent new code. This new code, and the attempts to maintain coherency with previous operating systems, will make Microsoft's task that much more difficult. If one maintains coherency, the product takes longer to get to the market, and it is more expensive because additional testing and software maintenance is required. If one leaves the legacy systems behind, the software can be more advanced, but this often requires additional hardware and the backlash of customers unable to use their legacy software. In both of these cases, the costs are being transferred to the customer. Microsoft passes their added costs of additional testing and software maintenance to the consumer through increased software prices. If Microsoft leaves the legacy software behind, the Navy will probably realize increased hardware needs, and

possibly additional software requirements to accommodate the replacement of legacy software. In either case, additional costs will be borne by the United States Navy.

In the author's opinion, it appears that the effort to maintain coherency with the numerous third-party drivers and other aspects of the operating system is catching up with Microsoft. As a result, Microsoft has chosen not to carry along the legacy in favor of greater reliability. In her article, *Win 2000 Will Drop a Lot of Legacy Code*, Morgan relays that in an attempt to improve reliability and stability in Windows 2000, Microsoft will remove a fair amount of its legacy code behind. In fact, as Jim Allchin, senior vice president and Windows 2000 team leader said, "When push comes to shove, we'll choose reliability over compatibility." (Morgan, 1999) As Allchin said, "...the company had identified third-party drivers, virtual device drivers and rogue Dynamic Link Libraries as the main sources of frequent system crashes and 'blue screens of death.'" (Morgan, 1999) What does this mean for the United States Navy? It means that the United States Navy will have to migrate most, if not all, of their systems to Windows 2000 Pro, as well, in order to benefit from this reliability. However, this will cause increased costs due not just to the upgrade, but the rewrite of the legacy programs to Windows 2000 standards and the purchase of new hardware to accommodate Windows 2000. In the author's opinion, the United States Navy should take note of Gartner Group analyst Hayward's observations. As Hayward notes,

> Even in the software business, past success is no guarantee of future prospects. Microsoft's dominance will be constrained by the legacy of its architectural choices and the ever-increasing difficulty of extending its scope. Signs of these pressures are already apparent. Because of delays and discontinuities in product releases, organizations that put their IT strategies into autopilot with 'buy Microsoft' policies will be disadvantaged relative to their more discriminating competitors. (Hayward, 1999)

In the author's opinion, if the Navy is to have the best hardware and software, it should allow the purchase of "best of breed" products in future information system

acquisition policy. If these products happen to be Microsoft, so be it, but to set a vendor-based standard for future information system deployments has the possibility of stagnating the Navy and allowing competitors—the enemy—to have the advantage.

D. SINGLE VENDOR-BASED STANDARDS DO NOT NECESSARILY INCREASE INTEROPERABILITY

The Naval Virtual Internet policy states that, "Applications selections are based upon functionality and approved Naval standards, which may extend to selection of single vendor commercial off the shelf (COTS) product offerings to ensure interoperability." (NVI, 1997) However, in the author's opinion, the premise that a single vendor-based standard will provide interoperability is incorrect when these standards are applied, in a practical sense, in the United States Navy. Single vendor product offerings do not necessarily ensure interoperability in an organization the size of the United States Navy. At this point one might ask, "How can you *not* have interoperable systems with the same vendor standard?" Interoperability will not necessarily be provided because the United States Navy will rarely have the same version of the same vendor-based standard throughout the entire Navy, unless the Navy decides to buy a particular version of software and never upgrade. In a small organization, the whole organization can be upgraded at one time so that every desktop has the same version of the same software. The enormous size of the United States Navy precludes such wholesale replacement, and as a result, different versions of the software will permeate the organization, thus maintaining some level of the Navy's current interoperability problems. While interoperability problems will be reduced somewhat, they will probably not be eliminated through the selection of a single vendor-based standard.

1. Definition of Interoperability

While much has been said about interoperability, no formal definition has been introduced in this thesis. The *Information Technology Standards Guidance (ITSG)* takes its interoperability definition from the *Joint Chiefs of Staff Publication One (JCS Pub 1).* JCS Pub 1 defines interoperability as, "The ability of systems, units or forces to provide services to, and accept services from, other systems, units or forces, and to use the services so exchanged to enable them to operate effectively together." (ITSG, 1998) This fairly broad definition of interoperability would allow computer programs to be "interoperable" if they could save their data in a format that was compatible with other computer programs—thus making a single vendor-based standard unnecessary. A more narrow definition of interoperability is offered by the Defense Information Systems Agency (DISA), Center for Standards Librarian. DISA defines interoperability as "The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users." (DISA, 1999) In this more restrictive definition, "exchanged directly" is interpreted by the author to mean that no conversions must take place for interoperability to exist. Information is "exchanged satisfactorily," in the author's opinion, if that information is in a usable form at the final destination. In a small organization, this definition of interoperability can be easily achieved through the purchase of the same version of the same vendor-based standard application. No conversion must take place, files do not need to be saved in another format, and files can be exchanged in a satisfactory and reliable manner. In a larger organization, like the United States Navy, it is too costly to supply the whole organization with the same version of the same computer application or operating system at the same time. As a result, the file will need some conversion to a "standardized" format that is transmitted on a "standardized" protocol in order to be interoperable. Consequently,

"interoperability," as defined in these constricted terms, is not even obtainable unless the whole organization has the *same version* of the same vendor-based standard. However, as a matter of practicality, the whole United States Navy will rarely have the same version of the same vendor-based standard. As a result, a conversion will most likely take place in order to satisfactorily exchange data. Since a conversion is likely required to obtain interoperability, in the author's opinion, a vendor-based standard becomes unnecessary.

2. The "Lasagna Effect"

Due to the enormous size of the Navy and the excessive costs associated with information technology hardware and software, information systems can not be summarily replaced across the United States Navy at one time. As a result, the United States Navy will rarely have a situation where everyone in the Navy will have the same computer hardware, the same version of the same standard operating system, the same version of a standardized email program, or the same version of office automation system software. For the whole Navy to accomplish such a task, they would have to make a wholesale purchase of a particular computer platform and a wholesale purchase of a particular software version and not upgrade until all units in the Navy had that particular hardware or software version. As a matter of practicality, the Navy would not likely adopt such a policy. The speed with which software versions are developed and distributed to market, the increased functionality in these products, and the changing needs of the Navy all drive the Navy towards the purchase of newer versions of software and hardware. In fact, sometimes an upgrade in the operating system software itself requires an upgrade in application software or hardware, as is often the case when upgrading older Windows 95/98 computers to Windows NT.

As a result of these factors, and others, it is the author's opinion that the Navy will always have a heterogeneous mix of hardware and software versions, even though they

have standardized on particular vendor applications and computer platforms. There will probably never be a homogeneous hardware and software standard in the Navy in all practicality. It is just too expensive and too complicated to carry out in an organization the size of the United States Navy. Fortunately, the Navy is not alone in this predicament. The commercial sector has also found that it can not make wholesale purchases and distribute information systems throughout their entire organizations at one time. As research and consulting company CooperComm Inc. reported in *A Transition Based End User Computing Financial Model*, "New end-user technology is no longer being replaced at once across an entire organization. This is too costly. It now propagates through an organization creating 'The Lasagna Effect'...a heterogeneous mix of technologies." (Crabb, 1997) This "Lasagna Effect" creates different versions of software and different hardware combinations even though a single vendor might be named as the standard.

For example, if the United States Navy standardizes on Microsoft Office, it will have some in the Navy who have Microsoft Office Professional 95, some with Microsoft Office Professional 97, and some who have Microsoft Office Professional 2000. This homogeneous software product standard is matched by a "Lasagna Effect" of heterogeneous software versions as depicted in Figure 7.3 below.

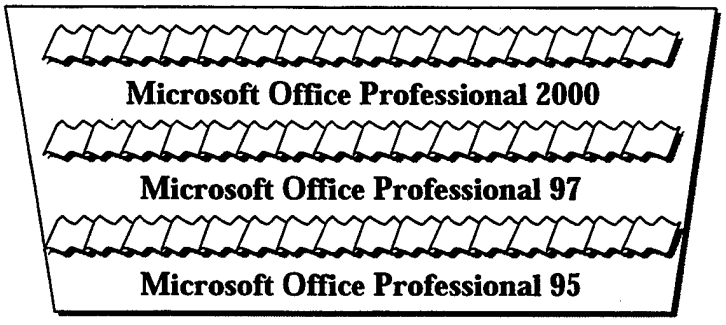

Figure 7.3: Lasagna Effect for Applications

Once most of the Navy has Microsoft Office 2000, Office 200x will be the new standard and some of the Navy will have Office 2000 and the rest will have the newest version of the software—Office 200x. As a result, a conversion will have to be made, or files will have to be saved in a specified format to ensure that the files are interoperable. Furthermore, if the document is required to look the same at the destination as at its origin, then both computers must have the same fonts installed. If they have different fonts, then the document will undergo font conversion. This font conversion may have unintended consequences. Depending on the font, some characters might not display as intended and the formatting might change to accommodate these new fonts. If this conversion has to take place anyway, it is the author's opinion that there is no practical reason to have a homogeneous vendor-based software standard. The Navy could leverage competition and purchase two different Office Automation System Software packages and still be interoperable. A management policy that calls for documents to be saved in a specified format using specified fonts would allow for increased interoperability in the word processing document realm. These policies can sometimes be set as a default in their respective programs so the end user does not have to remember to perform the conversion. Similar management policies could also be adopted for other software applications so interoperability can be maintained and competition can be leveraged to reduce prices.

The "Lasagna Effect" is even more pronounced in the operating system software arena. If one were to look strictly at the Microsoft operating systems in the United States Navy, one would find a number of different Microsoft operating systems, spanning several different versions. If one looks at the history of the Microsoft operating systems, as detailed in Table 7.1 below, it is not hard to see why the Navy has so many different versions of the Microsoft operating system.

Table 7.1: History of Microsoft Windows

Date	Operating System
November 20, 1985	Windows 1.0 released
April 2, 1987	Microsoft announces Windows 2.0
May 22, 1990	Windows 3.0 released
April 6, 1992	Windows 3.1 released
October 27, 1992	Windows for Workgroups 3.1 released
August, 1993	Windows NT 3.1 released
November 8, 1993	Windows for Workgroups 3.11 released
September 6, 1994	Windows NT 3.5 released
May, 1995	Windows NT 3.51 released
August 24, 1995	Windows 95 released
August 24, 1996	Windows NT 4.0 released
June 25, 1998	Windows 98 released

From Condron, 1999.

The Navy currently has about half of the operating systems described above scattered about the service. IT-21 requires that the Navy standardize on Windows NT and that should help get rid of some of these operating systems, but just because the Navy standardizes on Windows NT, does not mean it will all be running the same version of Windows NT. If one were to look at what the IT-21 standardized operating system might look like after it has been implemented, in the author's opinion, it would look something like Figure 7.4, taking the "Lasagna Effect" into consideration.

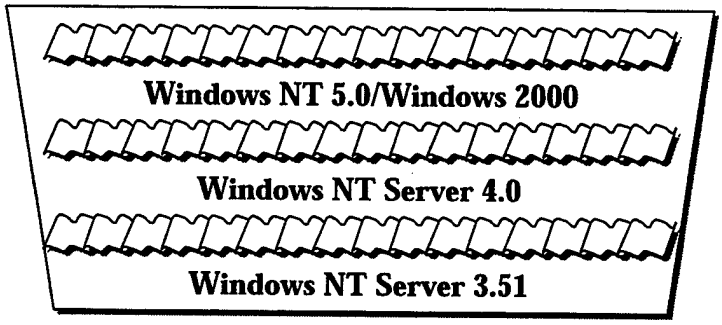

Figure 7.4: Lasagna Effect for Operating Systems

The Navy would have some commands, ships, and units with Windows NT Server version 3.51, some with version 4.0, and some with version 2000. Each new

version of this operating system has new functionality and its own set of operational procedures, training requirements, and troubleshooting provisions.

In the author's opinion, the conversion to Windows 2000 from Windows NT version 4.0 is going to be much more difficult than the conversion from version 3.51 to version 4.0 of NT. "The mostly new code in Windows 2000 makes it such a different beast than its NT 4.0 predecessor that corporate developers had better brace themselves..." explains Gaudin in her article, *Win 2000's Dirty Secret: Most Applications Must be Rebuilt.* "Most of their existing applications will have to be rebuilt, or at least revised, to make them compliant." (Gaudin "Win2000", 1999) According to Daniel Kusnetzky, an analyst at International Data Corporation, "Eighty percent of the code in Windows 2000 is new...If that's not a new operating system, I'm not sure what is. With the Windows platform, each migration from one version to the next has been tough. This will be tougher." (Gaudin "Win2000", 1999) In all practicality, this is a new operating system compared to version 4.0 of Windows NT. How is this new version of NT, Windows 2000, different from a network operating system supplied by a different vendor? In the author's opinion, with 80 percent of the code new, it is not much different from an offering by another vendor. With the "Lasagna Effect" the Navy will still have the added costs of training people, determining trouble shooting techniques, and establishing procedures for these distinct versions of the Navy's vendor-based standardized operating system. With the "Lasagna Effect" the Navy will probably never have a truly homogeneous information system—even though it standardized on one operating system.

3. Standards Adoption-Implementation Lag Time

There are many reasons why a single vendor-based standard will not eliminate the Navy's interoperability problems. Of those, the lag time from standards adoption to implementation plays an immense part. By the time a standard is decided upon and

adopted, to the time that the information reaches the fleet and the fleet actually gets the funding to implement that standard, there will probably already be a new version of the product released by the software vendor. This lag time from standards formulation, to adoption, and implementation is so substantial that it ensures new versions of hardware and software will be released prior to the fleet being able to implement that standard. Take the IT-21 standard email solution, Microsoft Exchange, as an example. The Navy standardized on Microsoft Exchange version 5.0, but Microsoft Exchange version 5.5 is now the current version. As a result, those just getting the funding to buy Exchange for their ships, squadrons, and units, will buy a version of Exchange that may, or may not, be compatible with its previous version. The rapidity with which commercial-of-the-shelf software is revised and brought to market has put the Navy in a precarious position. The Navy will have those in the fleet who have the current "published" version of the software standard, those with the "just released by the vendor but not formally adopted by the Navy" version, and those with the "past" version of a particular software product, depending on when in the products lifecycle the organization buys the product. It takes too long and it is too expensive to deploy software throughout the fleet unilaterally. As a result, the United States Navy will have a difficult time creating a truly homogeneous software environment.

In 1965, Gordon Moore observed that the performance of a memory chip roughly doubled that of its predecessor every 18-24 months. This observation, which came to be known as "Moore's Law," showed how computing power could rise exponentially over relatively brief periods of time. This trend has continued and "Moore's Law" has been applied to many facets of the Information Technology field because it has been remarkably accurate in forecasting future performance. Moore's Law is commonly applied to advances in the microprocessor. Table 7.2 below shows the history of the Intel Microprocessor.

Table 7.2: History of the Intel Microprocessor

Processor	Date	Processor	Date
Pentium III (500, 450 MHz)	1999	IntelDX4	March 7, 1994
Intel Celeron (300 MHz)	June 8, 1998	Intel486 SL	November 9, 1992
Pentium II (350, 400 MHz)	April 15, 1998	IntelDX2	March 3, 1992
Intel Celeron (266 MHz)	April 15, 1998	Intel486 SX	April 22, 1991
Pentium II (333 MHz)	January 26, 1998	Intel486 DX	April 10, 1989
Pentium II (300, 266, 233 MHz)	May 7, 1997	Intel386 SL	October 15, 1990
Pentium Pro (200 MHz) 1 MB L2 cache	August 18, 1997	Intel386 SX	June 16, 1988
Pentium Pro (200, 180, 166, 150 MHz)	November 1, 1995	Intel386 DX	October 17, 1985
Pentium (233 MHz) w/MMX	June 2, 1997	80286	February 1982
Pentium (200, 166 MHz) w/MMX	January 8, 1997	80186	1982
Pentium (200 MHz)	June 10, 1996	8088	June 1979
Pentium (166, 150 MHz)	January 4, 1996	8086	June 8, 1978
Pentium (133 MHz)	June 1995	8085	March 1976
Pentium (120 MHz)	March 27, 1995	8080	April 1974
Pentium (90, 100 MHz)	March 7, 1994	8008	April 1972
Pentium (75 MHz)	October 10, 1994	4004	November 15, 1971
Pentium (60, 66 MHz)	March 22, 1993		

From "*Intel Microprocessor*," 1999.

If one looks at the dates that these processors were introduced and the requirements for IT-21, it will become apparent why the Navy will probably never have a homogeneous computer hardware environment. The IT-21 policy requires, at a minimum, a 200 MHz Pentium Pro CPU for a standard desktop PC, a 150 MHz Pentium CPU for a standard laptop, and Dual 166 MHz Pentium CPU's for a Windows NT file server depending on the specific needs of the network. The 150 MHz and 166 MHz Pentium CPU's were introduced in January 4, 1996. The 200 MHz Pentium Pro CPU was introduced on November 1, 1995. The *Information Technology for the 21st Century*

policy was released on March 30, 1997 and the deadline for its compliance is December of 1999. If a command standardized on the 200 MHz Pentium Pro machine, the technology would be four years old by the time of the deadline for final compliance with IT-21. Furthermore, if they did not buy all of their computers at the time of the release of the IT-21 policy, then they would probably not be able to buy Pentium Pro CPU's because no retailer would be selling them. Figure 7.5 below details the significant milestones of the IT-21 policy and the lifecycle of IT hardware in the United States Navy.

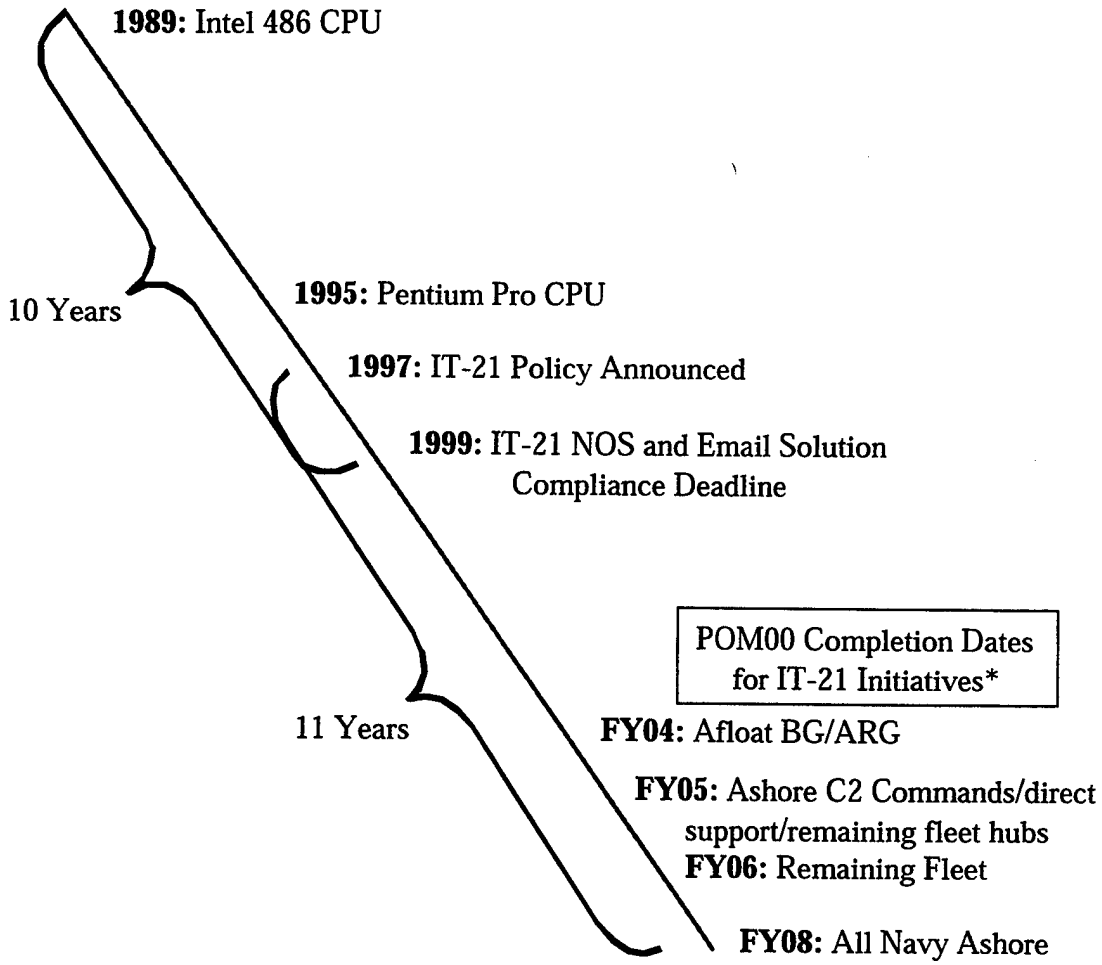

Figure 7.5: United States Navy Hardware Lifecycle

*After Mayo, 1998.

As a matter of practicality, if the Navy still has Intel 486 based computers in ships, squadrons, and units in the Navy, it is holding on to technology that is 10 years old. The computer industry recognizes a three-year lifecycle for computer equipment. This three-year lifecycle represents at least two generations of technology if "Moore's Law" holds true. Our 10 plus year old equipment represents at least seven generations of technology. Less powerful processors, like those found in Intel 286 and 386 machines, will only increase this technology gap. This technology gap and product refresh lifecycle doesn't even take into consideration the problems of getting the funding for these information systems. With the Planning, Programming, and Budgeting System, it takes at least two years to get items into the Navy Program Objectives Memorandum (POM), get them approved, and then get them added to the President's Budget. POM 00, which was developed in FY98, contains six years of the United States Navy spending plan. The fiscal year dates on the timeline in Figure 7.5 represent the completion dates for the IT-21 initiatives as described in a C4I Day brief by Rear Admiral Richard W. Mayo. It will take seven years for the completion of all IT-21 initiatives for afloat Battle Groups (BG) and Amphibious Readiness Groups (ARG) and 11 years for all ashore units to implement their IT-21 initiatives from the date of standards adoption in March of 1997. This additional funding delay increases the overall lag-time from standards adoption to final implementation. According to Rear Admiral Richard W. Mayo's (CNO N6B) C4I Day brief on November 3, 1998 titled *Delivering an Integrated Solution*, the Fiscal Year 1999 Afloat Funding for IT-21 has a 50.5 million-dollar shortfall with a 298.9 million afloat cost. The Fiscal Year 2000 Afloat Spend Plan for IT-21 has a 133.9 million-dollar shortfall with a 475.0 million afloat cost. (Mayo, 1998) These IT-21 cost shortfalls represent just the United States Navy afloat units. Other shortfalls could hurt shore units as well, and will once again, likely increase the time from standards adoption to final implementation. When it comes time to set standards, in the author's opinion, the Navy

should be prepared to live with these standards for at least the next 10 years, which represents the realistic and practical lifecycle of information systems in the Navy, if other means are not found to decrease this lag time.

The alacrity with which these microprocessors have originated has added to the difficulty in providing for a homogeneous hardware standard. As Gartner Group analyst Knox asserts, "...standardizing on any given platform for more than six months remains next to impossible. New technologies are being introduced on what seems to be a daily basis, and OEMs are forced to adopt these technologies quickly to remain competitive, further compressing product life cycles." (Knox, 1999) It is not just the CPU's that have changed in computer equipment. Hard drive sizes, random access memory requirements, CD-ROM speeds, chipsets on the motherboards, video cards, third party add-in cards, and other ancillary components have also changed and continue to change. These changes create literally hundreds of different hardware configurations in relatively short periods of time, even with a single vendor standard. While it is understood that these are just the minimum requirements, it is the author's opinion that the mere fact that the technology changes with such velocity, makes it almost impossible to have a homogeneous hardware standard and it is most surely impractical.

E. INTEROPERABILITY WITHOUT VENDOR-BASED STANDARDS

Vendor-based standards are not required for fleet-wide interoperability in the United States Navy in the author's opinion. In fact, millions of transactions a day happen on the internet by people using a variety of computer platforms using a variety of different applications. Why are people able to use Unix/Linux, Macintosh, and Wintel PC's on the internet with a variety of different programs and still maintain interoperability? The standardization of the interfaces, protocols (TCP/IP), and document formats (.pdf/HTML/XML), has allowed for this interoperability. One of the most simple-to-understand examples of why vendor-standardization is not needed is

demonstrated with email. People can still send email to each other using a variety of email software packages from a variety of computer platforms—as long as the software conforms to some standardization at the level of protocols and data representation. That's where protocols such as SMTP and IMAP, and data standards such as ASCII, XML/HTML, MIME, and Portable Document Format (.pdf) formats come in. For example, if a person sends an email from one MIME-compatible email client on a Unix computer to another MIME-compatible email client on a Wintel PC, full interoperability is the result. Likewise, if one puts an attachment to the email that is in ASCII, XML/HTML, or .pdf, from a Macintosh computer and sends that to someone on a Wintel PC, that person gets full interoperability, and they get that interoperability for free because the browsers for HTML/XML and .pdf files are free. These examples are demonstrated in Figure 7.6 below.

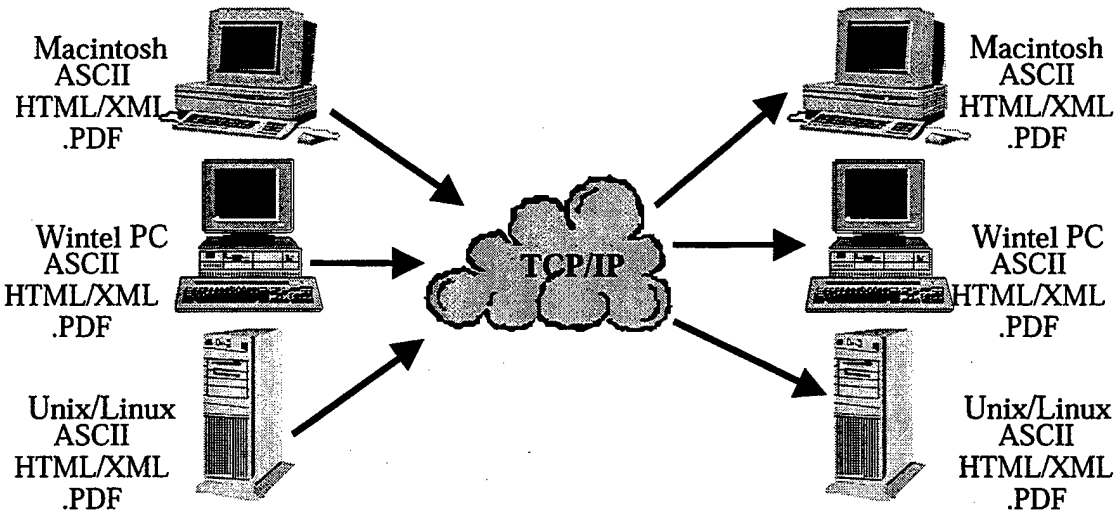

Figure 7.6: Interoperability Through Standardization of Protocols and Formats

So, in the author's opinion, as large buyers of Information Systems the Navy's objective should be to encourage, cajole, or force, industry to develop software with open

standards (MIME is a good example—all major GUI-based email clients conform), or to encourage the development of a market for building conversion products. The ITSG agrees with this concept when it states, "All things being equal, products that comply with open system standards are the preferred choice." (ITSG, 1998)

F. DUAL PLATFORM SUPPORT COST "PREMIUM?"

In 1995, Gartner Group conducted an analysis of the technical support costs associated with a heterogeneous computing environment. More specifically, they examined the impact of a dual platform computing environment (Macintosh and Windows 3.xx) on technical support costs. The study was based on detailed surveys of 67 companies representing a wide variety of industries and installed base sizes. While this study might be old in an information technology sense, it is the author's opinion that some of the principal findings and conclusions still hold true today, even though the names and faces of the computer platforms have changed. It is for this reason that this information is introduced in this thesis.

1. Theory

To understand the importance of the technical support cost "premium" concept, it is important to examine some of the theory surrounding this idea. If one were to endorse the idea that it costs more to support dual platforms across an enterprise, then one would expect to see increased technical support costs per computer platform unit in that enterprise. This increased cost would be reflected as a technical support cost "premium," and it would reflect that cost "peak" associated with some mix of these platforms. If there is truly a technical support cost "premium" associated with a dual platform environment, one would expect to see "technical support costs per unit rise, peak at a certain maximum and then begin to drop again, as the mix of platforms is varied from

one extreme to the other." (Gartner Group, 1995) The technical support cost "premium" concept is graphically depicted in Figure 7.7 below.

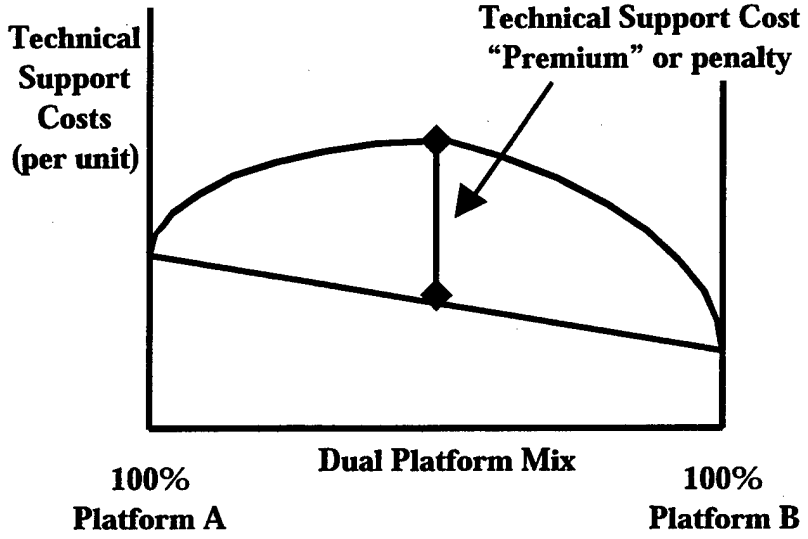

Figure 7.7: Technical Support Cost "Premium" Concept

From Gartner Group, 1995.

2. Results

While it is intuitive to think that there would be such a dual platform support cost "premium," the Gartner Group study showed that "In general, there is no detectable technical support cost *'premium'* associated with dual platform (Macintosh and Windows 3.xx) environments, compared to single platform environments." (Gartner Group, 1995) In fact, the study revealed that "...overall support costs decline as the percentage of Macintosh systems in the environment increases, and similarly, support costs increase as the percentage of Windows 3.xx systems increases." (Gartner Group, 1995) While this last statement may or may not hold in today's computing environment, it is important to recognize that it might be the case that a dual platform enterprise would not increase

technical support costs. In the author's opinion, before the Navy concedes to what its intuition might tell it, further examination should be performed to determine if there is, in all actuality, a dual support cost "premium" in today's Navy computing environment.

There is a lot of evidence to explain why there would not be an increase in technical support costs in a heterogeneous computing environment. The interviewees in this study were able to successfully control the support costs in this heterogeneous environment by providing homogeneity at crucial architectural layers in their organizations. These layers included the networking layer (file and print services), and application layer. In the Gartner Group study, "Successful support managers consistently indicated that the critical factors in their success were the use of cross-platform applications and single networking services. In the application area, Microsoft Office was typically singled out; for networks, TCP/IP and NFS appeared with surprising frequency." (Gartner Group, 1995) The particular application and the particular protocol do not matter in this case. As long as both platforms can support the application and the protocol, then technical support costs will not increase and interoperability can be maintained.

3. Importance of Strict Management and Best Practices

The remarkable and somewhat counter-intuitive results in the Gartner Group study *Technical Support Costs in "Dual Platform" Computing Environments*, were a result of good management by the organizations surveyed, not the particular technology that they used. As the study notes,

> Although the benefits achieved by the flexible use of multiple desktop systems have long been acknowledged, there has always been the belief that there was a support cost penalty associated with diversity. Our observations would indicate that a significant number of organizations have learned where to concentrate their management efforts to avoid these extra cost penalties. (Gartner Group, 1995)

It is this "management effort" which is the truly telling portion of this study, and in the author's opinion, a portion that continues to be true in today's information technology environment. No matter what platform one standardizes on, the management of those platforms is one of the keys to reducing costs. Table 7.3 below describes the support ratio required for those platforms that were tightly managed and those loosely managed in the study.

Table 7.3: Average Support Ratios per Platform

Windows 3.xx		Macintosh	
Loosely Managed	Tightly Managed	Loosely Managed	Tightly Managed
1 FTE/15 Units	1 FTE/77 Units	1FTE/24 Units	1 FTE/90 Units

FTE – Full Time Equivalent
From Gartner Group, 1995.

In this case, the reader will notice that the platform did not make as much a difference in the ratio of support required as the level of management applied to those platforms. The fact that tightly managed platforms require less personnel to manage is a key factor in reducing the total cost of ownership of Navy information systems. In the author's opinion, the information system policy after IT-21 should concentrate on this management aspect. While the IT-21 policy does a lot to delineate what hardware and software to use in the Navy computing architecture, it does little to direct the Navy on the policies and administration of those systems. It is this type of management that provides the cost reductions sought after by that policy.

4. Conclusions of Dual Platform "Premium" Study

Finally, the dual platform study confirmed that, "...a closer look, as suggested by our interviewees, indicates that there is no such thing as a homogeneous environment in

the real world." (Gartner Group, 1995) This observation is consistent with the "Lasagna Effect" stated earlier in this chapter and is consistent with reality. Wintel PC, Unix/Linux, and Macintosh "environments" contain two or three generations of hardware, spanning several different models. The use of third-party add-in cards in Windows environments means there are literally hundreds of different combinations of hardware and drivers present in just a "pure" Windows environment.

> As a result, a closer look reveals that the explanation for many of the results reported here is simply that *every environment is heterogeneous*...Thus, the explanation for the missing 'dual-platform penalty' in this study may be that it is actually present in every environment, even so-called 'pure' ones. As a result, its impact on technical support costs is built in from the beginning, and the minor perturbation introduced by having two environments present in a particular situation does not make any difference. (Gartner Group, 1995)

In all practicality then, almost every computing "environment" is heterogeneous in today's computing realm. In the author's opinion, the Navy should embrace this heterogeneity, and the benefits of its diversity, so it can learn how to better manage its heterogeneous information systems.

G. CHAPTER SUMMARY

The *Information Technology Standards Guidance* recognizes the compressed lifecycles of information technology systems, and the need for incremental change, when it affirmed,

> The pace of IT innovations has increasingly shortened the life spans of IT products. The technical complexity of products is also increasing. The high mobility of forces and rotation of support personnel make this product turnover and complexity especially acute for the Navy and Marine Corps....DON IM/IT strategy will change at a reasonable rate—one that keeps us current but minimizes changeover disruption. Use of the Information System Domain concept will allow for incremental change across the Naval enterprise while maintaining enterprise-wide interoperability." (ITSG, 1998)

However, in the author's opinion, the "Lasagna Effect" will prevent enterprise-wide interoperability despite the Information System Domain concept, and the lag time from standards adoption to implementation will keep the Navy from getting these new standards implemented in a timely manner. Just as a Carrier Battle Group can not steam faster than its slowest ship, the Navy can not expect to be interoperable with ships and squadrons that do not have the same information system resources as other units.

In the author's opinion, the Navy needs to allow for the acquisition of "best of breed" products with significantly compressed acquisition times than it currently has. As Paul G. Kaminski, former Undersecretary of Defense for Acquisition and Technology has said:

> The issue is not only cost. The lives of our soldiers, sailors, marines and airmen may depend upon shortened acquisition cycle times as well. In a global market everyone, including our potential adversaries, will gain increasing access to the same commercial technology base. The military advantage goes to the nation who has the best cycle time to capture technologies that are commercially available, incorporate them in weapon systems and get them fielded first. ("Applying COTS," 1999)

In working to solve the Navy's interoperability problems in a cost-effective manner, in the author's opinion, the Navy should examine the guidelines set by Gartner Group. In selecting open operating systems, Gartner Group recommends,

> Select technology that fits the standard profile and information systems requirements and supports all facets of the organization as well as the customer. Profile-based procurement is the best way to ensure enterprise-wide interoperability and portability. However, if products cannot be found that meet the profile, then a non-open system product may be the most appropriate. If this is the situation, avoid single vendor-controlled technologies, choosing more open technologies wherever possible. (Magee, 1998)

The single vendor-based standard runs counter to this recommendation. In the author's opinion, the Navy should take a practical and critical look at the Navy's

homogeneous vendor-based standard to determine if it is really the direction the Navy should proceed in its future information system acquisition policy.

VIII. RECOMMENDATIONS AND CONCLUSIONS

A. INTRODUCTION

In his article, *The Importance of Standards*, Gartner Group Datapro analyst Taylor explains, "...[Standards] often, if not always, represent a less than optimal design and implementation solution for any given, specific need." (Taylor, 1997) In the author's opinion, if the Navy is to become a more productive organization as a result of using information systems, system administrators should be given the latitude to purchase the hardware and software applications that will allow the Navy to be productive in its many and diverse operating environments. On initial inspection, standardization arguments make sense for the reduction of cost and the increase in interoperability. However, this thesis has demonstrated that a single vendor standard, and in particular Microsoft Windows NT, will not necessarily provide for that increase in interoperability or reduced costs. A homogeneous vendor-based standard also ignores the benefits diversity gives the end user, the one who actually does the work. More importantly, it ignores the pending disaster of common cause failures or single points of failure in the Navy information system architecture. In the military, common cause failures will put the lives of its sailors and soldiers at risk, and with the availability of Windows NT compared to other operating systems and platforms, the Navy will be putting them at even greater risk.

To mitigate the concerns or risks introduced in this thesis associated with a homogeneous vendor-based standard, this chapter will offer an alternative computing architecture, void of products and vendors. An object-oriented computing architecture will provide fleet-wide interoperability, will allow the use of legacy equipment and applications, promotes platform independence, and will help reduce costs. When establishing standards policy, in the author's opinion, the Navy should be concerned with

the *interface* standards and *the commonality of information exchange*, not vendors or products. If the Navy standardizes at these interface levels, it can create an object-oriented approach to architecture, where a change in one part of the architecture will not affect another part of the architecture. It will also decrease the dependence on vendor-based proprietary products and allow platform independence, thus freeing up the Navy to buy information systems in a competitive environment. This should decrease the overall risk to the United States Navy and ultimately allow greater flexibility for the adoption of future unknown technology advances.

B. OBJECT ORIENTED ARCHITECTURE

1. Computer Architectures

There are several types of computing architectures that have evolved through the years. When the computer was born, the predominate computing architecture in use was the mainframe architecture. With this architecture, all the business logic and intelligence was contained in a central host computer. Dumb terminals were used to access the host computer to perform work. When the personal computer arrived on the scene, PCs became networked, and the file sharing architecture took form. In this architecture, shared files are downloaded and run on the user's desktop. Both the business logic and the data were transferred to the end users desktop to perform the work. This architecture created great demands on network resources and used up copious amounts of limited network bandwidth.

In an attempt to establish a more efficient approach and overcome the limitations of file sharing architectures, the client/server architecture was developed. This computing architecture provided a versatile and modular infrastructure designed to improve interoperability, scalability, and flexibility. In this architecture, a database server replaced the file server and allowed direct answers to queries through the use of a

relational database management system. Processing management was effectively split between the end user system and the database server. This reduced the traffic on the network by providing just the response to the query vice a transfer of a complete file as was required under the file sharing architecture.

Client/server architectures are described in terms of tiers. The paragraph above describes a 2-tier client/server architecture. This is the model the United States Navy has put to practice on many ships, units, and squadrons throughout the Navy. The 2-tier environment has seen success due in large part to the proliferation of tools that aid in database integration and rapid application development. However, the 2-tier model has several weaknesses that make the development and maintenance of such applications much more expensive.

One of the main disadvantages of a 2-tier client/server architecture is that the business logic and presentation logic for an application accumulates on the end users PC. Since that business logic is tied to an individual PC-program, it can not be reused. This poses a problem whenever the organization makes changes in their business logic. Every program that uses that logic must be changed to accommodate the new business logic. This causes added expense as each program that has been changed must undergo quality control to ensure it is implementing the business logic correct and is generating the desired results. Once the programs are tested, they have to be reproduced and distributed throughout the organization. This can be very expensive, complicated, prone to error, and time consuming. The 3/n-tier architectures endeavor to solve these problems. This goal is achieved primarily by moving the application logic from the client back to a server.

2. Three-Tier Architecture

In a 3-tier, or multi-tier architecture, a middle tier is added between the user interface on the client and that database server in an attempt to overcome the limitations

of the 2-tier architecture. This middle tier contains most of the business logic, provides a more object-oriented approach to the architecture, and enables programs to scale to meet the wider usage of an entire enterprise. Figure 8.1 below diagrams a 3-tier object-oriented computing architecture.

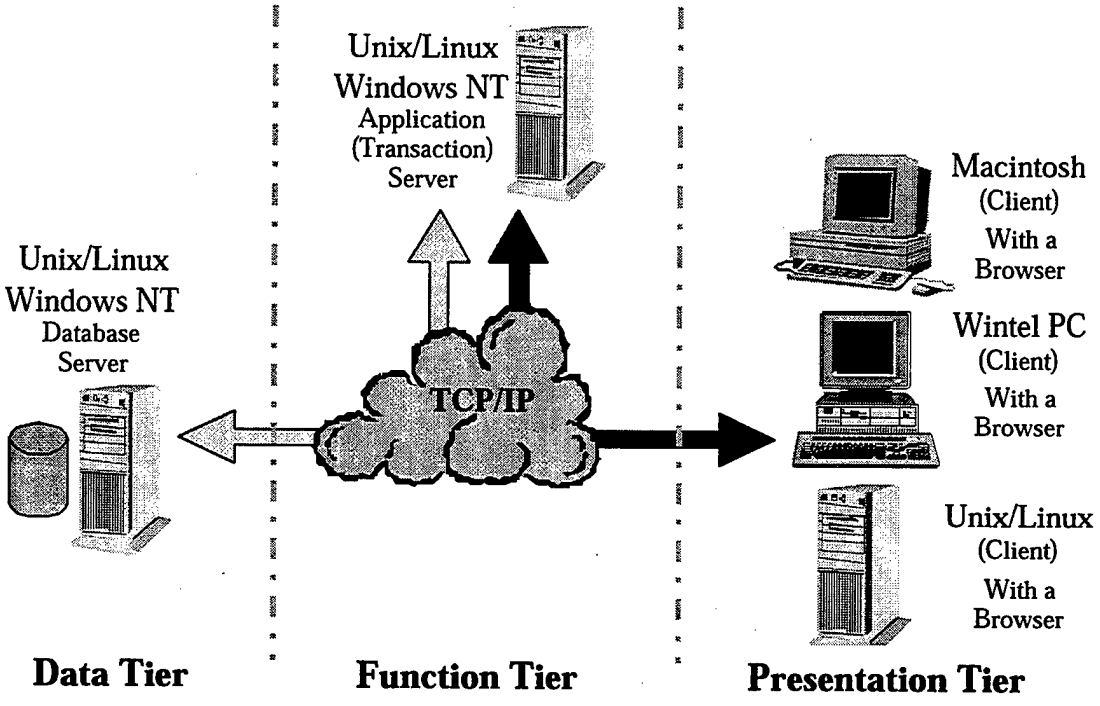

Figure 8.1: 3-Tier Object-Oriented Architecture

The key characteristic of a 3-tier client/server architecture is the separation of the computing environment into data, function, and presentation components, such that there are well-defined software boundaries or interfaces between each component. It is important to note that while the boundaries between tiers are logical, and it is possible to run all three tiers on the same physical machine, this architecture is often implemented on separate physical computers. Each part of the architecture is described below:

> *Data Tier* - This tier is responsible for storing the data required by the Function tier. Relational database systems, as well as older pre-existing

legacy database systems, can be used here. This tier has the same functionality in both 2 and 3-tier environments.

Function Tier – This tier is responsible for performing the main function or business logic of the application. This tier is not present in the 2-tier architecture and it protects the data in the data tier from direct access by the clients.

Presentation Tier – This tier is responsible for providing only the presentation of the information to the end user. This presentation is usually in the form of some graphical user interface that runs on the user's computer (e.g., web browser).

3. Advantages of 3-tier Architectures

The major advantages of a 3/n-tier architecture come from its object-oriented approach. The separation of the data, function, and presentation components, allow this architecture to promote the scalability, maintainability, and security of United States Navy software applications. Scalability is increased as this separation makes it easier to implement load balancing by allowing processes to be dynamically moved to other servers in the tier when bottlenecks in performance occur. With the implementation of web browsers as the presentation component, more clients in the organization have access to a wider variety of server applications. Applications are easier to maintain because the modification or replacement of software in one tier can be accomplished without affecting any of the other tiers. In addition, when changes occur and new programs have to be added, it is much easier and faster to change a few servers than to upgrade every end user PC in the organization with the new software. Furthermore, it is easier to build in redundancy and diversity into this type of architecture. Best of all, most of the changes that need to occur, are transparent from the end user's perspective. This should help decrease the costs required to train the end-users on using a particular software application. Furthermore, new business logic components can be developed and

integrated quicker because business objects can be reused. Testing can also be shorter because the data and presentation components have already been tested and do not require change. Finally, since the critical business processes, those that are the most sensitive and need to be most protected, are contained on a few servers vice thousands of clients, it is simpler to implement the security for this relatively few number of servers.

4. Types of 3-tier Architectures

There are numerous ways of implementing the middle tier of the 3-tier architecture. This tier can be used as a transaction processing monitor, an application server, or an Object Request Broker (ORB) to name a few. When this tier is used as a Transaction Processing monitor, transactions can be queued, scheduled, prioritized, and managed to their completion thus freeing up the client to perform other tasks. It also allows information to be pulled from a variety of data sources before returning the outcome to the end user. When the middle tier is used as an application server, those applications become more scalable, administration costs are reduced, and security efforts can be focused on the server. As an application server, this tier performs the business logic and data retrieval, and then provides the resulting information to the presentation component for display on the client's desktop. Finally, when this tier is used in an object request broker architecture, interoperability across languages, platforms, and applications can be achieved. It is this technology that holds the most promise for the United States Navy, as well as private enterprise.

The two main distributed object technologies that will fill this middle tier are the Common Object Request Broker Architecture (CORBA), an open systems standard, and Component Object Model (COM)/Distributed Component Object Model (DCOM), a Microsoft solution. "An important marker for government acceptance of CORBA came last year when DISA endorsed it as a preferred middleware standard for the Defense Information Infrastructure Common Operating Environment. A study conducted by

DISA compared CORBA to other middleware products—such as Microsoft Corp.'s Distributed Component Object Model and Open Group Ltd.'s Distributed Computing Environment—and came down on the side of CORBA." (Robinson, 1999) It is for this reason that CORBA will be proposed as the middleware solution for this object-oriented architecture. However, this architecture is not tied to the CORBA paradigm. The eXtensible Markup Language (XML) is also showing promise as middleware, and could be easily substituted to provide the same functionality and benefits of CORBA if that is the direction the market takes.

5. Common Object Request Broker Architecture (CORBA)

As Gartner Group analyst Altman (1998) states,

> While it is seductive to think that standards will emerge to eliminate the time and cost of application integration, this is unrealistic except in severely limited circumstances. Managers should embrace the inevitable semantic diversity of their application inventory and employ a broker-based integration strategy that can effectively manage the semantic transformation required to enable application integration. (Altman, 1998)

This broker-based integration strategy is provided by CORBA, the Common Object Request Broker Architecture. CORBA provides a standard way of creating interfaces that allow computer applications to communicate with one another no matter what language they were programmed in, what operating system they are running on, or where they are located on the network.

So how does CORBA work? The Object Request Broker (ORB) establishes a client/server relationship between objects by defining a standard interface by which applications communicate. When a client wants the server to perform some function, the ORB intercepts the call and finds an object locally, or on the network, that can perform the request. Once an object is found, it passes the object any parameters required for its operation, the object performs the function, and the ORB returns the results to the client.

All of the functions of the ORB are transparent to the end user, "...who have no need to know what software or computer system is used to generate the information they are looking for or where it is located on the network." (Robinson, 1999). They send a request and get an answer just as if it were being conducted on their own platform. One other component of the Common Object Request Broker Architecture is the Internet Inter-ORB Protocol (IIOP). This protocol provides the communication mechanism required to guarantee that all CORBA-compliant ORBs will be able to interact.

One of the main advantages of CORBA is its inclusion of standard application program interfaces. "That means applications can be developed without regard to changes in the IT infrastructure and can be plugged in as needed," and as a DISA spokesman said, "This will allow infrastructure and mission applications to evolve separately, supporting timely insertion of emerging products." (Robinson, 1999) So how long until this technology can be implemented in the Department of Defense? Bill Vass, director of technical services at the CIO's office within the Office of the Secretary of Defense has already conducted a proof of concept which showed that, "the architecture based on the CORBA standard worked, successfully communicating between the platforms that needed to coexist in the environment, including mainframe, Unix, Microsoft Windows NT and Windows 95 platforms." (Robinson, 1999) In the author's opinion, it is this type of object-oriented approach to architecture, vice vendors and products, which should be pursued if the Navy wants its architecture to be sustainable, interoperable, and cost effective.

C. STANDARDIZATION - DATA FORMATS AND TRANSMISSION PROTOCOLS

In order for the Client/Server model of computing to perform in a standardized and scaleable fashion, the ITSG states that, the interfaces must satisfy two basic criteria:

- Data element standardization between the end systems

- The interface between end systems and the network must be standardized (ITSG, 1998)

The Transmission Control Protocol/Internet Protocol (TCP/IP) is currently being used as the interface between end systems and the network. This is a fairly simple solution as the Internet has already solved this problem for the Navy. However, the Navy has yet to establish a policy for data element standardization. As a result, data element standardization will be the focus of this part of the chapter.

1. Data Element Standardization

A vendor-based standard does not provide data element standardization in an organization the size of the United States Navy, due in part, to such things mentioned earlier in this thesis—namely the "Lasagna Effect." If the Navy wants its information systems to be scalable and interoperable, it should establish a policy for data element standardization. When an information system standard is based on vendors and products, that standard must be carefully managed for each and every product in an organization's inventory. It is not sufficient to standardize on a product alone. For example, if an organization standardized their word processing functions to one product, Microsoft Word, they could not guarantee interoperability throughout the organization. Due to the "Lasagna Effect," they would have some with Microsoft Word 95, some with Microsoft Word 97, and some with Microsoft Word 2000. Microsoft Word 2000 can open and read Microsoft Word 95 and 97 files, but Microsoft Word 95 can *not* open and read Microsoft Word 97 and 2000 files. As such, the minimum required to ensure interoperability throughout the enterprise is a policy of least common denominator. The organization must keep track of their inventories and establish a product standard of the least common denominator—in this case, the Microsoft Word 95 version of their vendor standard. All files must be saved in that version in order to obtain interoperability throughout the organization. Once products are upgraded to newer versions of this vendor-based

standard, the least common denominator can be raised to Word 97 or Word 2000, whatever the case may be. Figure 8.2 below illustrates the data element standardization called for with an IT-21 vendor-based approach.

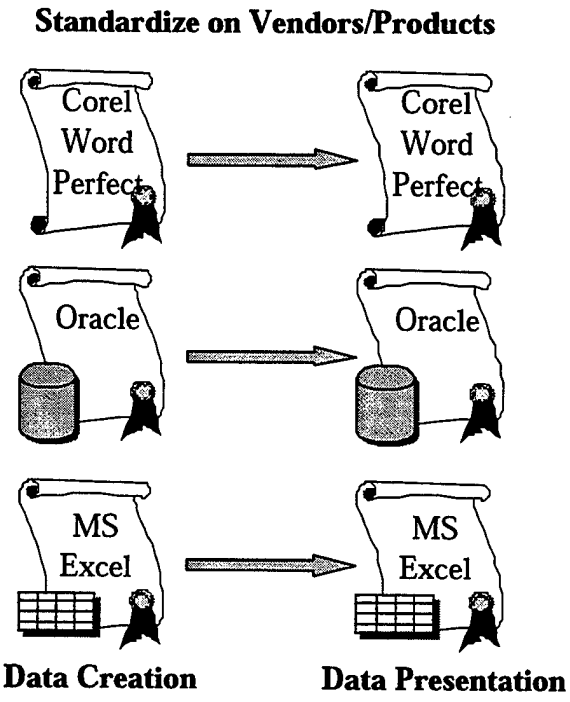

Figure 8.2: IT-21 Data Element Standardization

This approach will create an immense management burden and will require all organizations to have the same products for data presentation as they have for data creation. If an organization just needs to view a document, but does not need to edit that document and does not require any other functionality that the product offers, they still have to buy the product to view the document. This cost may not be that expensive with word processing programs, but when other more costly programs are entered into the equation, this cost increases exponentially. Furthermore, it is not just the cost of the software itself that affects the bottom line of the organization. These programs have to be

managed throughout the entire enterprise to ensure data element standardization, and this management function is often equal to or greater than the cost of the software itself.

In the author's opinion, if the Navy want to decrease costs, allow for central administration of databases and documents, and increase interoperability, it should think about data element standardization in terms of document creation and presentation. Just because a document is created by one program doesn't mean that product has to be viewed by that same program. If the Navy standardizes at the data presentation layer, any program can be used to create the document, and free platform-independent readers like web browsers (XML/HTML) and Adobe Acrobat Reader (.pdf) can be used to view the document. Figure 8.3 below illustrates the data element standardization with an open systems standards approach.

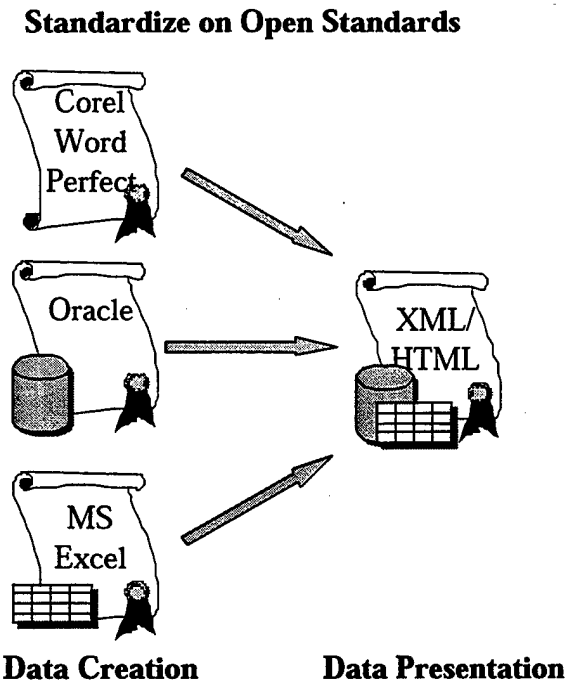

Figure 8.3: Data Element Standardization Using Open Standards

If the Navy uses presentation formats with open system platform-independent readers, an organization that wants to take advantage of the information on a particular database or in a particular document created by another organization, doesn't have to own the program that created that database or document. This gives the originating organization, who owns a database or document, ultimate authority or control to make changes to their data but still allows others in the enterprise the ability to view the data, and they can view that data for free. In the author's opinion, the Navy should stay common with industry and move as much of the Navy's applications as practical to the web using an XML compatible web browser.

2. eXtensible Markup Language (XML)

In the 1970s, the Standard Generalized Markup Language (SGML) emerged as a standard for defining the structure and content of an electronic document. Hyper Text Markup Language (HTML) and eXtensible Markup Language (XML) are both derivatives of this language, but where HTML is a common syntax for expressing the presentation of data, XML is a common syntax for expressing the structure in data. As a result, XML can be used to indicate the content, meaning, or use of a particular piece of data. By separating structure and content from presentation, the same XML source document can be written once, and read many times by a variety of XML compliant computer platforms and communications devices.

Like HTML, XML was developed for the Web and is platform-independent. This characteristic of platform independence is of great benefit to the Navy. This will allow a more object-oriented approach to the Navy computer architecture and allows legacy system data and applications the ability to continue to be used until funding can be procured to modernize these systems. In fact, the Department of Defense is already experimenting with XML to do just that. As Don O'Brien, project manager for research and development at the Defense Logistics Agency claims, "I am exploring the idea of

using XML for connections into legacy systems...It's a clean and powerful way to do that." (Lazar, 1999). With the use of this object-oriented approach to standardization, a change in one part of the organization does not effect a change in another part of the organization. With the use of XML/HTML as a presentation and content standard, vendor lock-in and platform dependence are minimized and problems with proprietary formats become irrelevant. This platform independence will allow legacy systems to be accommodated and will provide flexibility for rapid changes in industry. It is this type of data element standardization, vice vendor-based standardization, which the author believes is required to increase interoperability and reduce costs.

D. CONCLUSION

The goal of the Information Technology Standards Guidance (1998) is to provide guidance to managers, integrators, and designers to:

- Reduce the dependence on proprietary solutions.
- Offer the best potential for scalability, adaptability and market acceptance while minimizing the financial loss-of-service consequences of choosing/replacing non-optimal components.
- Allow for controlled growth and upgrades as requirements change and expand. (ITSG, 1998)

Although one of the ITSG's goals is to reduce the dependence on proprietary solutions, a single vendor-based standard does just the opposite. The adoption of this vendor-based standard will lock the United States Navy into this vendor for years to come, thus increasing the Navy's dependence on this vendor proprietary solution. Second, choosing one standard is a very risky proposition if the goal is to offer the best potential for scalability, adaptability, and market acceptance. If the market decides to deviate from the chosen standard, the Navy will be left with a "homogeneous" infrastructure that will need to be wholly replaced to make it adaptable and bring it in line with the market. The military experienced a similar situation when it chose Ada as its

standard computer programming language and the market went the direction of C and C++. If more than one language were chosen as the programming language standard, then theoretically, roughly half of the programs would have to be rewritten to conform to commercial practices. With one standard however, all the programs would have to be rewritten to fall in line with commercial practices. Finally, a single vendor-based standard does not allow for controlled growth and upgrades as requirements change and expand. While the Navy might be able to change its requirements to conform to the standardized vendor-based solution, there might be another vendors offering that would fill the requirement with less effort and at a reduced price. As Gartner Group analyst Gartenberg explains,

> Enterprises shopping for new applications should carefully review what competitors offer. It could be more complex and expensive to integrate non-Microsoft applications into a Microsoft environment, but it may be worth the additional initial investment to achieve certain functionality advantages and long-term savings. (Gartenberg "Microsoft", 1998)

With a single vendor standard, in the author's opinion, the Navy will not be able to pursue such an option and "best of breed" products will take the backseat to the standard.

Several items have been introduced throughout this thesis to describe the concerns or deficiencies the author identified with a vendor-based standard. Having a vendor-based standard forces client-side platform dependence and requires a custom client interface with frequent upgrades on hundreds of platforms. To enable an enterprise-level architecture that is both cost effective and provides fleet-wide interoperability, the author believes the Navy should employ an object-oriented approach to its computing architecture. While this approach is by no means a silver bullet, it goes farther than a vendor-based standard in accommodating legacy computing equipment, allowing for future IT advances, providing reduced costs, and enabling fleet-wide interoperability. Hopefully, the inclusion of some of these ideas into the next generation of the Navy's

information system standardization policy will help reduce costs and increase fleet-wide interoperability.

LIST OF REFERENCES

A Microsoft Takeover At NASA/Johnson Space Center. [Online] Available http://www.ghg.net/madmacs/Takeover.html, October 22, 1998.

AberdeenGroup, Inc. *Total Cost of Ownership - Monkey See, Monkey Do*. [Online] Available http://www.aberdeen.com/cgi-bin/rf.cgi, March 7, 1999.

AFCEA/Naval Institute Expo Convention Remarks as prepared for Admiral Archie R. Clemins, USN Commander in Chief, United States Pacific Fleet San Diego Convention Center. January 24, 1997.

Altman, R. "Standards Won't Eliminate Need for Application Integration," *GartnerAdvisory: Research and Advisory Services*. Research Note. Tactical Guidelines. November 20, 1998.

Altman, R., and T. Austin. "A New Architecture Must Cost-Justify a Technology Shift." *Gartner Advisory: Research and Advisory Services*. Research Note. Tutorials. November 3, 1998.

Apple Online Store [Online] Available http://store2.apple.com/, March 17, 1999.

Applying COTS Products and Services to Major Defense Programs. [Online] Available http://www.mc.com/COTS_folder/cots_mtb/cots_mtb.html, April 20, 1999.

Arnavas, D. and W. Ruberry. *Government Contract Guidebook*. Second edition. Limited Softcover Version with 1998 Supplement. Federal Publications Inc. Copyright 1994.

Barkan, J., and N. MacDonald. "Windows 2000: Renamed, Repackaged NT, at a Higher Price," *Gartner Advisory: Research and Advisory Services*. Monthly Research Review. December 25, 1998.

Behar, R. "Who's Reading Your E-Mail?" *Fortune Magazine*. February 3, 1997.

Bona, A. "Microsoft Licensing: More Than One Way to Play Monopoly," *Gartner Advisory: Research and Advisory Services*. Monthly Research Review. October 1, 1998.

Bona, A., and M. Welch. "Microsoft OSs: Count the Cost of a Prior Version." *Gartner Advisory: Research and Advisory Services.* Research Note. Strategic Planning. May 11, 1998.

Brady, T. *IS 3112 Class Notes.* Naval Postgraduate School. 1998.

Brewin, B. "Microsoft Probes Unix Territory." *Federal Computer Week,* Volume 13, Number 14. May 10, 1999.

Brewin, B. "U.S. Navy Brings Command and Control to NT." *Windows NT World.* Number 1. December 1998.

Burns, C. *Virus Threatens NT Nets: Microsoft, Network Associates Team on Fix.* [Online] Available http://www.nwfusion.com/news/0111remote.html, January 11, 1999.

Cappuccio, D., B. Keyworth, and W. Kirwin. *Total Cost of Ownership: The Impact of System Management Tools,* [Online] Available http://gartner12.gartnerweb.com/public/static/software/rn/00031136.html, September 17, 1996.

Cebrowski, A. [VADM, USN], "Information Technology for the 21st Century (IT-21): Accelerating the Revolution," CNO-N6 PowerPoint Brief. June 13, 1997.

Cebrowski, A. [VADM, USN] and J. Garstka. "Network-Centric Warfare: Its Origin and Future." *U.S. Naval Institute Proceedings.* January, 1998.

CERT/CC Incident Notes. [Online] Available http://www.cert.org/incident_notes, July 17, 1998.

Chronological History of Windows NT Related. [Online] Available http://www.jwntug.or.jp/misc/japanization/history.html, February 10, 1999.

Condron, F. *Microsoft Windows History.* [Online] Available http://www.conitech.com/windows/wintime.html, March 2, 1999.

Crabb, D. *Macs Still Hold the Edge in Total Cost of Ownership. MacWeek.* [Online] Available http://macweek.zdnet.com/mw_1117/op_manager.html, April 25, 1997.

Cusumano, M. and R. Selby. "How Microsoft Builds Software." *Communications of the ACM.* Volume 40, Number 6. June 1997.

Davis, J. "Final Evaluation Report, Microsoft, Inc., Windows NT Workstation and Server version 3.5 with U.S. Service Pack 3." *National Computer Security Center.* Report No. CSC-FER-95/003. Library No. S243,073. April 29, 1996.

Diederich, T. "NATO Web Site hit by Yugoslav Hackers." *ComputerWorld.* [Online] Available http://www.computerworld.com/home/news.nsf/CWFlash/9904014nato, April 01, 1999.

Distributed Computing Chart of Accounts: The New Gartner Group TCO Model. [Online] Available http://microsoft.com/technet/tco/chart/chart.rtf, 1998.

Fitzpatrick, K. "Platform Availability Data: Can You Spare a Minute?" *GartnerAdvisory: Research and Advisory Services.* Research Note. Decision Framework. October 29, 1998.

Foley, M. "Enterprise Licenses: Be Very Afraid." *ZDNet.* [Online] Available http://www.zdnet.com/sr/stories/column/0,4712,2153008,00.html, October 22, 1998.

Foley, M. "New Security Flap Over Windows NT," *ZDNN.* [Online] Available http://www.zdnet.com/zdnn/stories/zdnn_display/0,3440,2140612,00.html, September 23, 1998.

Gartenberg, M. *Beyond the Numbers: Common TCO Myths Revealed,* [Online] Available http://gartner12.gartnerweb.com/public/static/software/rn/00060318.html, March 2, 1998.

Gartenberg, M., "Microsoft Dominance Need Not Intimidate IS Managers Who Plan Well." *Gartner Advisory: Research and Advisory Services.* Inside Gartner Group. September 2, 1998.

Gartner Group. *Technical Support Costs in "Dual Platform" Computing Environments.* Gartner Group Consulting Services. October 10, 1995.

Garvey, M. "The Hidden Cost of NT." *Information Week Online.* [Online] Available http://www.informationweek.com/692/92iuhid.htm, July 20, 1998.

Gaudin, S. "Beta 3 Fixes Tackle Win 9x Migration." *ComputerWorld.* [Online] Available http://www.computerworld.com/home/print.nsf/all/99022292AE, February 19, 1999.

Gaudin, S. "Win 2000's Dirty Secret: Most Applications Must be Rebuilt. " *ComputerWorld.* [Online] Available http://www.computerworld.com/home/print.nsf/all/99021590D6, February 15, 1999.

Harreld, H. "Hill Probes Mac-PC Controversy." *Federal Computer Week.* [Online] Available http://www.fcw.com/pubs/fcw/1997/0609/nasa.htm, June 9, 1997.

Hayward, S., et. al. "Constraints on Microsoft: The Hidden Factor." *Gartner Advisory: Research and Advisory Services.* Research Note. Strategic Planning Assumption. January 5, 1999.

Hess, M. and B. Redman. "The Elements of IT Transition." *Gartner Advisory: Research and Advisory Services.* Commentary. January 27, 1998.

Hoyland, A. and M. Rausand. *System Reliability Theory: Models and Statistical Methods.* John Wiley and Sons, Inc., 1994.

Intel Microprocessor Quick Reference Guide. [Online] Available http://www.galaxy.mb.ca/intelcpu.htm, March 22, 1999.

Interpose, Inc./IDC, "What is Total Cost of Ownership." *C/S Solution Advisor TCO Management Source,* 1997.

Knox, K. "Intel Desktop Configurations: Winter 1999 Update." *Gartner Advisory: Research and Advisory Services.* Research Note. Technology. January 29, 1999.

Lazar, G. "The XML Factor." *Federal Computer Week.* Volume 13, Number 9. April 5, 1999.

Lieberman, R. "Protests Protect Procurement System: Process is Safety Valve for Bidders." *Federal Computer Week,* Volume 13, Number 5. March 8, 1999.

Red Hat Linux. [Online] Available http://www.redhat.com/appindex/Applications/, March 8, 1999.

Machlis, S. "Military Beefing Up Its Hacker Defenses," *Computerworld,* Volume 31, Number14, CW Publishing Inc., 1997.

Magee, S. "Operating System Standards." *Gartner Group Datapro.* June 4, 1998.

Mayo, D. [RADM]. *C4I Day: Delivering an Integrated Solution.* PowerPoint Presentation. November 3, 1998.

McDonald, C. *The Security Implication of IT-21.* [Online] Available http://www.chips.navy.mil/chips/archives/98_apr/Chris.htm, August 1, 1998.

McGuckin, P. "The Benefits and Perils of 'Good Enough' Computing." *GartnerAdvisory: Research and Advisory Services.* Research Note. Tactical Guidelines. October 1, 1998.

McNee, B. et al. *The Industry Trends Scenario: Delivering Business Value Through IT,* [Online] Available http://gartner12.gartnerweb.com/public/static/software/rn/00065194.html, April 30, 1998.

Merritt, C. *Novell Extends Directory Leadership Across Major Platforms with NDS for Linux.* [Online] Available http://corp.novell.com.au/press/archive/1999/05/pr99053.html, May 18, 1999.

Messmer, E. "NT 4.0 Flunks Cryptography Test: Another Service Pack Fix and Interoperability Woes for Users are the Results." *Network World.* January 11, 1999.

Microsoft Online Store, [Online] Available http://shop.microsoft.com/store/home/homepage.asp, March 8, 1999.

Morgan, C. *Win 2000 Will Drop A Lot Of Legacy Code.* [Online] Available http://www.computerworld.com/home/news.nsf/CWFlash/9904165win2klegacy, April 16, 1999.

National Aeronautics and Space Administration, Office of Inspector General, Inspections and Assessments. Inspection Report: Johnson Space Center Information Technology Equipment Replacement. [Online] Available http://www.hq.nasa.gov/office/oig/hq/inspections/g-96-017.html, November 7, 1996.

Notes About the Wide Spread NT Denial of Service Attack that Occurred on March 2nd and 3rd, 1998. [Online] Available http://u6.mit.edu/afs/net.mit.edu/admin/www/network/BSOD-03041998.html, January 18, 1999.

Ohlson, K. "Defense lags in computer security, report charges." *Computerworld.* [Online] Available

http://www.computerworld.com/home/news.nsf/CWFlash/9903232military, March 23, 1999.

Orenstein, D. "Retailer Commits to Linux in 250 Stores." *ComputerWorld.* [Online] Available http://www.computerworld.com/home/print.nsf/all/9902159106, February 15, 1999.

PC Week Online Staff. "Microsoft's Ballmer: NT 5.0 Has 'A Long Way to Go." *PC Week Online.* October 23, 1998.

Raymond, E. *Frequently Asked Questions about Open Source.* [Online] Available http://www.opensource.org/faq.html, March 12, 1999.

Robinson, B. "The ORB Slowly Rises: The CORBA Middleware Standard Gains Functionality and Grows Increasingly Popular." *Federal Computer Week.* Volume 13, Number 13. May 3, 1999.

Russell, D., and G. Gangemi. *Computer Security Basics.* O'Reilly and Associates, Inc., 1991.

Scott, D., P. McGuckin, and C. Claunch. "HP's '5nines:5minutes':Ups the Ante for High Availability." *GartnerAdvisory: Research and Advisory Services.* Research Note. Events. September 22, 1998.

Shapiro, C., and H. Varian. *Information Rules: A Strategic Guide to the Network Economy,* Harvard Business School Press, Copyright 1999.

Silver, M. "Understaffing on NT Servers Leads to Loss of Employees and Higher Ownership Costs." *Gartner Advisory, Research and Advisory Services.* Point-to-Point. July 31, 1998.

Sliwa, C. "Net Reliability Hinges on Web Site Architecture." *Computerworld.* Volume 33, Number 35. August 30, 1999.

Smith, R. "NT's Top Security Problems," "Protect Your Passwords." *Windows NT Magazine,* October 1998.

Smith, T. "On The Register: Why Mac OS X Server?" *MacWEEK.com.* [Online] Available http://macweek.zdnet.com/1999/03/07/registerwed.html, March 10, 1999.

Spanbauer, S. "Software Bugs Run Rampant." *PC World.* [Online] Available http://www.pcworld.com/pcwtoday/article/0,1510,8844+1+0,00.html, January 1999.

Stoll, C. *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage.* Simon & Schuster Inc., 1990.

Symantec Web site, [Online] Available http://shop.symantec.com/, March 17, 1999.

Systems Engineering Management Guide. Defense Systems Management College. Chapter 16, 1983.

Taylor, L. "The Importance of Standards." *Gartner Group Datapro.* 14 October 1997.

Thompson, E. "Justifying Windows NT: Too Much Monkey Business." *Gartner Advisory: Research and Advisory Services.* Research Note. Decision Framework. September 8, 1998.

United States. *Annotated ITMRA 1996, Division E-Information Technology Management Reform. (Public Law 104-106)* [Online] Available http://www.dtic.mil/c3i/cio/references/itmra/itmra.Annot.html, October 10, 1998.

United States. Department of Defense. *C4I for the Warrior: The Joint Vision for C4I Interoperability.* January 1998.

United States. Department of Defense. CINCPACFLT Pearl Harbor, HI, *Information Technology for the 21st Century,* United States Navy, 300944ZMAR97 (ALPACFLT 008/97).

United States. Department of Defense. Defense Information Systems Agency (DISA), Center for Standards Librarian. *Definition of Interoperability.* [Online] Available http://www-library.itsi.disa.mil/org/fed_std/html/dir-019/_2838.htm, April 7, 1999.

United States. Department of Defense. DON CIO ITSG Integrated Process Team. *Information Technology Standards Guidance.* United States Navy. Version 98-1.1. June 15, 1998.

United States. Department of Defense. Naval Virtual Internet Integrated Process Team, *Naval Virtual Internet (NVI): Functional Architecture and Concept of Operations, Draft for comment (Revision 7b).* United States Navy. December 11, 1997.

United States. Department of Defense. Office of the Inspector General. *Statement For The Record Eleanor Hill, Inspector General, Department Of Defense, Before The Subcommittee On Readiness And Management Support Senate Committee On Armed Services On Acquisition Reform In The Department Of Defense.* Report Number 99-117. [Online] Available http://www.dodig.osd.mil/fo/99-117.pdf, March 31, 1999.

United States. *Federal Acquisition Regulations Part Six (FAR, PART 6)—Competition Requirements.* FAC 97–10. January 4, 1999.

United States. *Title 10 United States Code Sec. 2304 (10 USC 2304). Competition Requirements.* http://www4.law.cornell.edu/uscode/10/2304.html, March 25, 1999.

Valloppillil, V., and J. Cohen. *Linux OS Competitive Analysis: The Next Java VM (Microsoft Confidential).* v. 1.00. Microsoft Corporation. August 11, 1998.

Valloppillil, V. *Open Source Software: A (New?) Development Methodology (Microsoft Confidential).* v. 1.00. Microsoft Corporation. August 11, 1998.

Verton, D. "House Blasts DOD Over Savings Claims." *Federal Computer Week.* Volume 13, Number 5. March 8, 1999.

Verton, D. "IG Questions DOD Awards." *Federal Computer Week.* Volume 13, Number 11. April 19, 1999.

Weiss, G. "Windows NT Conference Survey Results." *Gartner Advisory: Research and Advisory Services.* Inside Gartner Group. July 30, 1997.

Weiss, G. "Comparing Linux to Windows NT and Commercial Unix." *GartnerAdvisory: Research and Advisory Services.* Research Note. Decision Framework. November 10, 1998.

Wilson, J. *Is There A COTS Backlash Growing In The Military?* [Online] Available http://www.pollux.com/defenseweb/1996/sept96/cots!.htm, April 20, 1999.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center. 2
   8725 John J. Kingman Road, STE 0944
   Fort Belvoir, VA 22060-6218

2. Dudley Knox Library 2
   Naval Postgraduate School
   411 Dyer Road
   Monterey, CA 93943-5101

3. Professor Dan C. Boger 1
   CS Dept, Code CS/CC
   Naval Postgraduate School
   Monterey, CA 93943

4. Professor Hemant K. Bhargava, ... 1
   SM Dept, Code IS/BH
   Naval Postgraduate School
   Monterey, CA 93943

5. Professor Theodore G. Lewis 1
   CS Dept, Code CS/LT
   Naval Postgraduate School
   Monterey, CA 93943

6. LT Travis J. Trupp 5
   11 Bodwell Street
   Brunswick, ME 04011

7. Rear Admiral John A. Gauss 1
   Space and Naval Warfare Systems Center
   53560 Hull Street
   San Diego, CA 92152-5001

8. LT Randy Shaffer. 1
   Deputy Chief Information Officer
   Naval Medical Center Portsmouth
   620 John Paul Jones Circle
   Portsmouth, VA 23708-2197

9. LT Christine Mankowski 1
   Head, IRMD
   Naval Hospital
   Camp Lejune, NC 28547-0100